Systemverwaltungshandbuch: Netzwerkdienste

Teilenr.: E22297
August 2011

ORACLE

Copyright © 2002, 2011, Oracle und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065, USA.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

111013@25097

Inhalt

Vorwort 37

Teil I Netzwerkdienste – Themen 43

1 Netzwerkdienst (Übersicht) 45
Themen für Oracle Solaris 10 Update 10 45
Perl 5 46
Zugang zur Perl-Dokumentation 46
Perl-Kompatibilitätsprobleme 47
Änderungen an der Solaris-Version von Perl 47

2 Verwalten von Webcache-Servern 49
Network Cache and Accelerator (Übersicht) 49
Webserver in Verbindung mit SSL-Protokoll (Secure Sockets Layer) 50
Verwalten von Webcache-Servern (Übersicht der Schritte) 51
Planung für NCA 52
Systemanforderungen für NCA 52
NCA-Protokollierung 52
Interpositionsbibliothek für Dämon-Unterstützung des Tor-Servers 52
Unterstützung für mehrere Instanzen 53
Verwalten der Zwischenspeicherung von Webseiten (Aufgaben) 53
▼ So aktivieren Sie die Zwischenspeicherung von Webseiten 53
▼ So deaktivieren Sie die Zwischenspeicherung von Webseiten 56
▼ So aktivieren oder deaktivieren Sie die NCA-Protokollierung 56
So laden Sie die Socket-Dienstprogramm-Bibliothek für NCA 57
▼ So fügen Sie einen neuen Port dem NCA-Service hinzu 57
▼ So konfigurieren Sie einen Apache 2.0-Webserver, um den SSL-Kernel-Proxy zu

verwenden 58
▼ So konfigurieren Sie einen Sun Java System-Webserver, um den SSL-Kernel-Proxy zu verwenden 60
Verwenden des SSL-Kernel-Proxy in Zonen 62
Zwischenspeicherung von Webseiten (Referenz) 63
NCA-Dateien 63
NCA-Architektur 64

3 Zeitorientierte Services 67
Uhrsynchronisierung (Übersicht) 67
Verwalten von Network Time Protocol (Aufgaben) 68
▼ So richten Sie einen NTP-Server ein 68
▼ So richten Sie einen NTP-Client ein 68
Verwenden anderer zeitorientierter Befehle (Aufgaben) 69
▼ So synchronisieren Sie Datum und Uhrzeit mit einem anderen System 69
Network Time Protocol (Referenz) 70

Teil II Zugriff auf Netzwerkdateisysteme – Themen 71

4 Verwalten von Netzwerkdateisystemen (Übersicht) 73
Neue Funktionen des NFS-Service 73
Änderungen in Solaris 10 11/06 73
Änderungen in Solaris 10 74
NFS-Terminologie 75
NFS-Server und -Clients 75
NFS-Dateisysteme 75
Informationen zum NFS-Service 76
Informationen zu Autofs 77
Funktionen des NFS-Service 77
Version 2 des NFS-Protokolls 77
Version 3 des NFS-Protokolls 77
Version 4 des NFS-Protokolls 78
Steuerung von NFS-Versionen 79
NFS-ACL-Unterstützung 80
NFS über TCP 80

NFS über UDP 80
Übersicht zu NFS über RDMA 81
Netzwerk-Sperren-Manager und NFS 81
NFS-Unterstützung für große Dateien 81
NFS-Client-Failover 81
Kerberos-Unterstützung für den NFS-Service 82
WebNFS-Unterstützung 82
RPCSEC_GSS-Sicherheitsvarianten 82
Solaris 7-Erweiterungen für die NFS-Einhängung 83
Sicherheitsaushandlung für den WebNFS-Service 83
NFS-Serverprotokollierung 83
Autofs-Funktionen 84

5 Verwaltung des Netzwerkdateisystems (Aufgaben) 85
Automatische Freigabe von Dateisystemen 86
▼ So richten Sie die automatische Freigabe von Dateisystemen ein 87
▼ So aktivieren Sie den WebNFS-Zugang 88
▼ So aktivieren Sie die NFS-Serverprotokollierung 89
Einhängen von Dateisystemen 90
▼ So hängen Sie ein Dateisystem während des Boot-Vorgangs ein 91
▼ So hängen Sie ein Dateisystem über die Befehlszeile ein 92
Einhängen mit dem Automounter 92
▼ So deaktivieren Sie große Dateien auf einem NFS-Server 93
▼ So verwenden Sie das clientseitige Failover 94
▼ So deaktivieren Sie den Einhängezugriff eines Clients 94
▼ So hängen Sie ein NFS-Dateisystem über eine Firewall ein 95
▼ So hängen Sie ein NFS-Dateisystem mithilfe einer NFS-URL ein 95
Einrichten von NFS-Services 96
▼ So starten Sie die NFS-Services 97
▼ So stoppen Sie die NFS-Services 98
▼ So starten Sie den Automounter 98
▼ So stoppen Sie den Automounter 98
▼ So wählen Sie andere NFS-Versionen auf einem Server aus 99
▼ So wählen Sie andere NFS-Versionen auf einem Client aus, indem Sie die `/etc/default/nfs`-Datei modifizieren 100

▼ Verwenden des `mount`-Befehls zum Auswählen anderer Versionen von NFS auf einem Client 101
Verwalten des Secure NFS-Systems 102
▼ So Richten Sie eine Secure NFS-Umgebung mit DH-Authentifizierung ein 102
WebNFS-Systemverwaltungsaufgaben 104
Planung für den WebNFS-Zugriff 105
So führen Sie Suchvorgänge mithilfe einer NFS-URL aus 106
So aktivieren Sie den WebNFS-Zugriff über eine Firewall 107
Aufgabenübersicht für die Autofs-Verwaltung 107
Übersicht der Schritte für die Autofs-Verwaltung 107
Verwenden der `/etc/default/autofs` -Datei zum Konfigurieren Ihrer autofs-Umgebung 109
▼ Konfigurieren der autofs-Umgebung mithilfe der `/etc/default/autofs`-Datei 109
Aufgaben zur Verwaltung von Maps 110
Modifizieren der Maps 111
▼ So modifizieren Sie die Master-Map 111
▼ So modifizieren Sie indirekte Maps 112
▼ So modifizieren Sie direkte Maps 112
Vermeiden von Einhängepunktkonflikten 112
Zugreifen auf Nicht-NFS-Dateisysteme 113
▼ So greifen Sie mit autofs auf CD-ROM-Anwendungen zu 113
▼ So greifen Sie mit autofs auf PC-DOS-Datendisketten zu 114
Zugreifen auf NFS-Dateisysteme mithilfe von CacheFS 114
▼ So greifen Sie mithilfe von CacheFS auf NFS-Dateisysteme zu 115
Anpassen des Automounters 115
Einrichten einer allgemeinen Ansicht von `/home` 116
▼ So richten Sie `/home` mit mehreren Home-Verzeichnis-Dateisystemen ein 116
▼ So konsolidieren Sie projektbezogene Dateien unter `/ws` 117
▼ So richten Sie verschiedene Architekturen ein, um auf einen gemeinsam genutzten Namespace zuzugreifen 119
▼ So unterstützen Sie nicht kompatible Client-Betriebssystemversionen 120
▼ So replizieren Sie gemeinsam genutzte Dateien auf mehreren Servern 120
▼ So wenden Sie Autofs-Sicherheitsbeschränkungen an 121
▼ So verwenden Sie eine Routine für den Zugriff auf öffentliche Dateien mit autofs 121
▼ So verwenden Sie die NFS-URLs mit autofs 122
Deaktivieren der autofs-Durchsuchfunktion 122

▼ So deaktivieren Sie vollständig die autofs-Durchsuchfunktion auf einem einzelnen NFS-Client ... 123
▼ So deaktivieren Sie die autofs-Durchsuchfunktion aller Clients ... 123
▼ So deaktivieren Sie die autofs-Durchsuchfunktion auf einem ausgewählten Dateisystem ... 124
Strategien für die NFS-Fehlerbehebung ... 124
NFS-Fehlerbehebungsverfahren ... 125
▼ So prüfen Sie die Konnektivität auf einem NFS-Client ... 126
▼ So prüfen Sie den NFS-Server per Remote-Zugriff ... 127
▼ So prüfen Sie den NFS-Service auf dem Server ... 128
▼ So starten Sie die NFS-Services neu ... 130
Feststellen, welcher Host den NFS-Dateiservice bereitstellt ... 130
▼ So prüfen Sie Optionen, die in Verbindung mit dem Befehl `mount` verwendet werden ... 130
autofs-Fehlerbehebung ... 131
Von `automount -v` generierte Fehlermeldungen ... 131
Verschiedene Fehlermeldungen ... 133
Weitere Fehler mit Autofs ... 134
NFS-Fehlermeldungen ... 135

6 Zugreifen auf Netzwerkdateisysteme (Referenz) ... 141
NFS-Dateien ... 141
`/etc/default/autofs`-Datei ... 143
Schlüsselwörter für die /etc/default/nfs-Datei ... 144
`/etc/default/nfslogd`-Datei ... 144
`/etc/nfs/nfslog.conf`-Datei ... 145
NFS-Dämonen ... 147
`automountd`-Dämon ... 147
`lockd`-Dämon ... 148
`mountd`-Dämon ... 149
`nfs4cbd`-Dämon ... 149
`nfsd`-Dämon ... 150
`nfslogd`-Dämon ... 150
`nfsmapid`-Dämon ... 151
`statd`-Dämon ... 159
NFS-Befehle ... 160
`automount`-Befehl ... 161

clear_locks-Befehl ... 161
fsstat-Befehl ... 162
mount-Befehl ... 162
umount-Befehl ... 169
mountall-Befehl ... 170
umountall-Befehl ... 170
share-Befehl ... 171
unshare-Befehl ... 177
shareall-Befehl ... 177
unshareall-Befehl ... 178
showmount-Befehl ... 178
setmnt-Befehl ... 179
Befehle zum Beheben von NFS-Problemen ... 179
nfsstat-Befehl ... 179
pstack-Befehl ... 181
rpcinfo-Befehl ... 182
snoop-Befehl ... 184
truss-Befehl ... 185
NFS über RDMA ... 185
Funktionsweise des NFS-Service ... 186
Versionsaushandlung in NFS ... 187
Funktionen in NFS-Version 4 ... 188
UDP- und TCP-Aushandlung ... 199
Aushandlung der Dateiübertragungsgröße ... 200
Einhängen von Dateisystemen ... 201
Funktionsweise der Option -public und der NFS-URLs beim Einhängen ... 202
Clientseitiges Failover ... 202
Große Dateien ... 205
Funktionsweise der NFS-Serverprotokollierung ... 205
Funktionsweise des WebNFS-Service ... 206
Funktionsweise der WebNFS-Sicherheitsaushandlung ... 207
WebNFS-Beschränkungen bei Verwendung eines Webbrowsers ... 208
Sicheres NFS-System ... 208
Secure RPC ... 209
Autofs-Maps ... 212
Master-Autofs-Maps ... 213

Direkte Autofs-Map 215
Indirekte autofs-Maps 217
Funktionsweise von autofs 219
Wie autofs durch das Netzwerk navigiert (Maps) 220
Wie autofs den Navigationprozess startet (Master-Map) 221
Autofs-Einhängeprozess 221
Wie autofs die nächsten schreibgeschützten Dateien für Clients auswählt (mehrere Speicherorte) 223
Autofs und Gewichtung 226
Variablen in einem Map-Eintrag 227
Maps, die sich auf andere Maps beziehen 228
Ausführbare autofs-Maps 229
Modifizieren, wie autofs im Netzwerk navigiert (Modifizieren von Maps) 230
Standardmäßiges Verhalten von autofs bei Verwendung von Name Services 230
Autofs-Referenz 232
Autofs und Metazeichen 232
Autofs und Sonderzeichen 233

Teil III SLP (Service Location Protocol) – Themen 235

7 SLP (Übersicht) 237
SLP-Architektur 237
Zusammenfassung des SLP-Konzepts 238
SLP-Agenten und Prozesse 238
SLP-Implementierung 240
Weitere SLP-Informationsquellen 242

8 Planen und Aktivieren von SLP (Aufgaben) 243
Überlegungen zur SLP-Konfiguration 243
Wann eine Neukonfiguration nötig ist 244
Verwenden von `snoop` zur Überwachung von SLP-Aktivitäten 244
▼ So verwenden Sie `snoop`, um SLP-Ablaufverfolgungen auszuführen 245
Analysieren einer `snoop slp`-Ablaufverfolgung 246

9 Verwalten von SLP (Aufgaben) 249
Konfigurieren von SLP-Eigenschaften 249
Grundelemente der SLP-Konfigurationsdatei 250
▼ So ändern Sie Ihre SLP-Konfiguration 251
Modifizieren der Häufigkeit von DA-Advertisements und -Erkennungen 252
Beschränken von UAs und SAs auf statisch konfigurierte DAs 253
▼ So beschränken Sie UAs und SAs auf statisch konfigurierte DAs 253
Konfigurieren der DA-Erkennung für DFÜ-Netzwerke 254
▼ So konfigurieren Sie die DA-Erkennung für DFÜ-Netzwerke 254
Konfigurieren des DA-Takts für häufige Partitionen 255
▼ So konfigurieren Sie den DA-Takt für häufige Partitionen 256
Entlastung des Netzwerks 257
Verwenden verschiedener Netzwerkmedien, Topologien oder Konfigurationen 257
Verringern von SA-Neuregistrierungen 257
▼ So reduzieren Sie SA-Neuregistrierungen 258
Konfigurieren der Multicast-Lebensdauereigenschaft 258
▼ So konfigurieren Sie die Multicast-Lebensdauereigenschaft 259
Konfigurieren der Paketgröße 260
▼ So konfigurieren Sie die Paketgröße 260
Konfigurieren des Nur-Broadcast-Routing 261
▼ So konfigurieren Sie Nur-Broadcast-Routing 262
Modifizieren von Zeitüberschreitungseinstellungen bei SLP-Suchanforderungen 262
Ändern der standardmäßigen Zeitüberschreitungseinstellungen 263
▼ So ändern Sie standardmäßige Zeitüberschreitungseinstellungen 264
Konfigurieren der Zufallswartezeit 265
▼ So konfigurieren Sie die Zufallswartezeit 265
Bereitstellen von Bereichen 267
Wann Bereiche zu konfigurieren sind 268
Überlegungen zum Konfigurieren von Bereichen 268
▼ So konfigurieren Sie Bereiche 269
Bereitstellen von DAs 270
Welchem Zweck dient die Bereitstellung eines SLP-DA? 270
Wann DAs bereitzustellen sind 272
▼ So stellen Sie DAs bereit 272
Wo DAs bereitzustellen sind 273
SLP und Multihoming 274

Multihoming-Konfiguration für SLP 274
Wann mehrere nicht gesteuerte Netzwerkschnittstellen zu konfigurieren sind 275
Konfigurieren mehrerer nicht gesteuerter Netzwerkschnittstellen (Übersicht der Schritte) 275
Konfigurieren der `net.slp.interfaces`-Eigenschaft 276
Proxy-Advertisement auf Multihomed-Hosts 277
DA-Bereitstellung und Zuweisung von Bereichsnamen 278
Überlegungen zum Konfigurieren von mehreren nicht gesteuerten Netzwerkschnittstellen 279

10 Integrieren von veralteten Services 281
Wann veraltete Services bekannt zu geben sind 281
Advertisement von veralteten Services 281
Modifizieren des Service 282
Bekanntgeben eines Service, der nicht SLP-fähig ist 282
SLP-Proxyregistrierung 282
▼ So aktivieren Sie die SLP-Proxyregistrierung 282
Verwenden der SLP-Proxyregistrierung für das Advertisement 283
Überlegungen zum Advertisement von veralteten Services 286

11 SLP (Referenz) 287
SLP-Statuscodes 287
SLP-Meldungstypen 288

Teil IV Mailservices – Themen 291

12 Mailservices (Übersicht) 293
Neue Funktionen der Mailservices 293
Änderungen in dieser Version 294
Änderungen in Solaris 10 1/06 294
Änderungen in Solaris 10 294
Weitere `sendmail`-Informationsquellen 295
Einführung in die Komponenten von Mailservices 295
Übersicht der Softwarekomponenten 295

Übersicht der Hardwarekomponenten 296

13 Mailservices (Aufgaben) 299
Übersicht der Schritte für Mailservices 299
Planen Ihres Mailsystems 301
Nur lokale Mail 301
Lokale Mails und eine Remote-Verbindung 302
Einrichten von Mailservices (Übersicht der Schritte) 304
Einrichten von Mailservices 304
▼ Einrichten eines Mailservers 305
▼ So richten Sie einen Mailclient ein 307
▼ So richten Sie einen Mailhost ein 309
▼ So richten Sie ein Mailgateway ein 310
▼ So verwenden Sie DNS mit `sendmail` 312
Ändern der sendmail-Konfiguration (Übersicht der Schritte) 313
Ändern der sendmail-Konfiguration 313
▼ So erstellen Sie eine neue `sendmail.cf`-Datei 314
Einrichten eines virtuellen Hosts 315
▼ So konfigurieren Sie die automatische Neuerstellung einer Konfigurationsdatei 315
▼ So verwenden Sie `sendmail` im offenen Modus 316
▼ So richten Sie SMTP zur Verwendung von TLS ein 317
▼ So verwalten Sie die Mailübermittlung mithilfe einer alternativen Konfiguration von `sendmail.cf` 322
Verwalten von Mailaliasdateien (Übersicht der Schritte) 323
Verwalten von Mailaliasdateien 325
▼ So initiieren Sie eine NIS+-`mail_aliases`-Tabelle 325
▼ So listen Sie die Inhalte der NIS+-`mail_aliases`-Tabelle auf 326
▼ So fügen Sie über die Befehlszeile Aliase in die NIS+-`mail_aliases`-Tabelle ein 327
▼ So fügen Sie Einträge durch Bearbeiten einer NIS+-`mail_aliases`-Tabelle ein 328
▼ So bearbeiten Sie Einträge in einer `mail_aliases`-NIS+-Tabelle 329
▼ So richten Sie eine `mail.aliases`-NIS-Map ein 330
▼ So richten Sie eine lokale Mailaliasdatei ein 331
▼ So richten Sie eine verschlüsselte Zuordnungsdatei ein 332
Verwalten des `postmaster`-Alias 333
Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte) 336

Verwalten der Warteschlangenverzeichnisse 336
▼ So zeigen Sie den Inhalt der Mailwarteschlange (`/var/spool/mqueue`) an 337
▼ So erzwingen Sie die Verarbeitung der Mailwarteschlange (`/var/spool/mqueue`) 337
▼ So führen Sie einen Teil der Mailwarteschlange (`/var/spool/mqueue`) aus 338
▼ So verschieben Sie die Mailwarteschlange (`/var/spool/mqueue`) 338
▼ So führen Sie die alte Mailwarteschlange (`/var/spool/omqueue`) aus 339
Verwalten von `.forward`-Dateien (Übersicht der Schritte) 339
Verwalten von `.forward`-Dateien 340
▼ So deaktivieren Sie `.forward`-Dateien 340
▼ So ändern Sie den `.forward`-Dateisuchpfad 341
▼ So erstellen und füllen Sie `/etc/shells` 342
Fehlerbehebungsverfahren und Tipps für Mailservices (Übersicht der Schritte) 342
Fehlerbehebungsverfahren und Tipps für Mailservices 343
▼ So prüfen Sie die Mailkonfiguration 343
So prüfen Sie Mailaliase 344
▼ So prüfen Sie die `sendmail`-Regellisten 345
So verifizieren Sie Verbindungen mit anderen Systemen 346
Protokollieren von Fehlermeldungen 346
Weitere Quellen für Maildiagnoseinformationen 347
Auflösen von Fehlermeldungen 348

14 Mailservices (Referenz) 351
Solaris-Version von `sendmail` 352
Zum Kompilieren von `sendmail` verwendete und nicht verwendete Flags 352
`MILTER`, Mailfilter-API für `sendmail` 354
Alternative `sendmail`-Befehle 354
Versionen der Konfigurationsdatei 354
Software- und Hardwarekomponenten von Mailservices 355
Softwarekomponenten 355
Hardwarekomponenten 363
Mailservice-Programme und -Dateien 366
Verbesserung des Dienstprogramms `vacation` 367
Inhalt des `/usr/bin`-Verzeichnisses 367
Inhalt des `/etc/mail`-Verzeichnisses 368
Inhalt des `/etc/mail/cf`-Verzeichnisses 369

Inhalt des /usr/lib-Verzeichnisses ... 372
Weitere Dateien, die für Mailservices verwendet werden ... 372
Interaktionen von Mailprogrammen ... 374
sendmail-Programm ... 375
Mail-Aliasdateien ... 379
.forward-Dateien ... 382
/etc/default/sendmail-Datei ... 384
Mailadressen und Mail-Routing ... 386
Interaktionen von sendmail mit Name Services ... 386
sendmail.cf und Maildomains ... 387
sendmail und Name Services ... 387
Interaktionen von NIS und sendmail ... 389
Interaktionen von sendmail mit NIS und DNS ... 389
Interaktionen von NIS+ und sendmail ... 390
Interaktionen von sendmail mit NIS+ und DNS ... 391
Änderungen in Version 8.13 von sendmail ... 392
Unterstützung für die Ausführung von SMTP mit TLS in Version 8.13 von sendmail ... 392
Zusätzliche Befehlszeilenoptionen in Version 8.13 von sendmail ... 397
Zusätzliche und überarbeitete Konfigurationsdateioptionen in Version 8.13 von sendmail ... 398
Zusätzliche und überarbeitete FEATURE()-Deklarationen in Version 8.13 von sendmail 399
Änderungen ab Version 8.12 von sendmail ... 400
Unterstützung für TCP-Wrapper ab Version 8.12 von sendmail ... 401
submit.cf-Konfigurationsdatei der Version 8.12 von sendmail ... 401
Zusätzliche oder eingestellte Befehlszeilenoptionen ab Version 8.12 von sendmail ... 403
Zusätzliche Argumente für die Optionen PidFile und ProcessTitlePrefix ab Version 8.12 von sendmail ... 404
Zusätzliche definierte Makros ab Version 8.12 von sendmail ... 405
Zusätzliche Makros ab Version 8.12 von sendmail ... 406
Zusätzliche MAX-Macros ab Version 8.12 von sendmail ... 407
Zusätzliche und überarbeitete m4-Konfigurationsmakros ab Version 8.12 von sendmail ... 408
Änderungen an der FEATURE()-Deklaration ab Version 8.12 von sendmail ... 408
Änderungen an der MAILER()-Deklaration ab Version 8.12 von sendmail ... 411
Zusätzliche Delivery Agents-Flags ab Version 8.12 von sendmail ... 412
Zusätzliche Gleichsetzungen für Delivery Agents ab Version 8.12 von sendmail ... 412

Zusätzliche Warteschlangenfunktionen ab Version 8.12 von `sendmail` 414
Änderungen für LDAP ab Version 8.12 von `sendmail` 414
Änderung am integrierten Mailer ab Version 8.12 von `sendmail` 416
Zusätzliche Regellisten ab Version 8.12 von `sendmail` 416
Änderungen an Dateien ab Version 8.12 von `sendmail` 417
`sendmail`-Version 8.12 und IPv6-Adressen in der Konfiguration 418

Teil V Serielle Vernetzung – Themen 419

15 Solaris PPP 4.0 (Überblick) 421
Solaris PPP 4.0 – Grundlagen 421
Solaris PPP 4.0-Kompatibilität 422
Zu verwendende Version von Solaris PPP 422
Weitere Informationen zu PPP 423
PPP-Konfigurationen und Terminologie 425
PPP-Einwahlverbindung – Übersicht 425
PPP-Standleitung – Übersicht 429
PPP-Authentifizierung 431
Authentifizierer und Authentifizierungsempfänger 432
PPP-Authentifizierungsprotokolle 432
Warum die PPP-Authentifizierung verwendet werden sollte 433
Unterstützung für DSL-Benutzer durch PPPoE 433
PPPoE – Übersicht 434
Teile einer PPPoE-Konfiguration 434
Sicherheit eines PPPoE-Tunnels 436

16 PLanen einer PPP-Verbindung (Aufgaben) 437
PPP-Gesamtplanung (Übersicht der Schritte) 437
Planen einer PPP-Einwahlverbindung 438
Vor dem Einrichten des Hinauswahlrechners 438
Vor dem Einrichten des Einwahlservers 439
Beispiel einer Konfiguration für eine PPP-Einwahlverbindung 440
Weitere Informationen zur PPP-Anwahl 442
Planen einer Standleitungsverbindung 442

Vor dem Einrichten der Standleitungsverbindung 442
Beispielkonfiguration für eine Standleitungsverbindung 443
Weitere Informationen zu Standleitungen 445
Planen der Authentifizierung zur Verwendung einer Verbindung 445
Vor dem Einrichten der PPP-Authentifizierung 445
Beispiele für PPP-Authentifizierungskonfigurationen 446
Weitere Informationen zur Authentifizierung 449
Planen der DSL-Unterstützung über einen PPPoE-Tunnel 450
Vor dem Einrichten eines PPPoE-Tunnels 450
Beispiel einer Konfiguration für einen PPPoE-Tunnel 452
Weitere Informationen zu PPPoE 454

17 Einrichten einer PPP-Einwahlverbindung (Aufgaben) 455
Wichtige Aufgaben zum Einrichten der PPP-Einwahlverbindung (Übersicht der Schritte) .. 455
Konfigurieren des Hinauswahlrechners 456
Aufgaben zum Konfigurieren des Hinauswahlrechners (Übersicht der Schritte) 456
Vorlagendateien für PPP-Einwahlverbindungen 457
Konfigurieren von Geräten des Hinauswahlrechners 457
▼ So konfigurieren Sie das Modem und den seriellen Port (Hinauswahlrechner) 458
Konfigurieren der Kommunikation des Hinauswahlrechners 459
▼ So definieren Sie die Kommunikation über die serielle Verbindung 460
▼ So erstellen Sie die Anweisungen zum Aufrufen eines Peers 461
▼ So definieren Sie die Verbindung mit einem bestimmten Peer 462
Konfigurieren des Einwahlservers 463
Aufgaben zum Konfigurieren des Einwahlservers (Übersicht der Schritte) 464
Konfigurieren von Geräten auf dem Einwahlserver 464
▼ So konfigurieren Sie das Modem und den seriellen Port (Einwahlserver) 464
▼ So legen Sie die Modemgeschwindigkeit fest 465
Einrichten von Benutzern der Einwahlservers 466
▼ So konfigurieren Sie Benutzer des Einwahlservers 466
Konfigurieren der Kommunikation über den Einwahlserver 467
▼ So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver) 468
Aufrufen des Einwahlservers 469
▼ So rufen Sie den Einwahlserver auf 469

18 Einrichten einer PPP-Standleitungsverbindung (Aufgaben) 471
Einrichten einer Standleitung (Übersicht der Schritte) 471
Konfigurieren von synchronen Geräten an der Standleitung 472
Voraussetzungen für das Einrichten von synchronen Geräten 472
▼ So konfigurieren Sie synchrone Geräte 472
Konfigurieren eines Rechners an der Standleitung 473
Voraussetzungen zum Konfigurieren des lokalen Rechners an einer Standleitung 473
▼ So konfigurieren Sie einen Rechner an einer Standleitung 474

19 Einrichten der PPP-Authentifizierung (Aufgaben) 477
Konfigurieren der PPP-Authentifizierung (Übersicht der Schritte) 477
Konfigurieren der PAP-Authentifizierung 478
Einrichten der PAP-Authentifizierung (Übersicht der Schritte) 478
Konfigurieren der PAP-Authentifizierung auf dem Einwahlserver 479
▼ So erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise (Einwahlserver) 480
Modifizieren der PPP-Konfigurationsdateien für PAP (Einwahlserver) 481
▼ So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver) 481
Konfigurieren der PAP-Authentifizierung für vertrauenswürdige Anrufer bzw. aufrufende Programme (Hinauswahlrechner) 483
▼ So konfigurieren Sie PAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer 483
Modifizieren von PPP-Konfigurationsdateien für PAP (Hinauswahlrechner) 485
▼ So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner) 485
Konfigurieren der CHAP-Authentifizierung 486
Einrichten der CHAP-Authentifizierung (Übersicht der Schritte) 487
Konfigurieren der CHAP-Authentifizierung auf dem Einwahlserver 488
▼ So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver) 488
Modifizieren der PPP-Konfigurationsdateien für CHAP (Einwahlserver) 489
▼ So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver) 490
Konfigurieren der CHAP-Authentifizierung für vertrauenswürdige Anrufer (Hinauswahlrechner) 490
▼ So konfigurieren Sie CHAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer 491
Einfügen von CHAP in die Konfigurationsdateien (Hinauswahlrechner) 492

▼ So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner) 492

20 Einrichten eines PPPoE-Tunnels (Aufgaben) 495

Wichtige Aufgaben zum Einrichten eines PPPoE-Tunnels (Übersichten der Schritte) 495

Einrichten des PPPoE-Clients 496

Voraussetzungen zum Einrichten des PPPoE-Clients 497

▼ So konfigurieren Sie eine Schnittstelle für einen PPPoE-Client 497

▼ So definieren Sie einen PPPoE-Zugangsserver-Peer 498

Einrichten eines PPPoE-Zugangsservers 500

▼ So richten Sie einen PPPoE-Zugangsserver ein 500

▼ So modifizieren Sie eine `/etc/ppp/pppoe` -Datei 501

▼ So beschränken Sie die Verwendung einer Schnittstelle auf bestimmte Clients 501

21 Beheben von allgemeinen PPP-Problemen (Aufgaben) 505

Lösen von PPP-Problemen (Übersicht der Schritte) 505

Tools zur Behebung von PPP-Problemen 506

▼ So rufen Sie Diagnoseinformationen aus `pppd` ab 507

▼ So aktivieren Sie die PPP-Fehlersuche 508

Lösen von Problemen im Zusammenhang mit PPP und PPPoE 509

▼ So diagnostizieren Sie Netzwerkprobleme 510

Allgemeine Netzwerkprobleme, von denen PPP betroffen ist 512

▼ So diagnostizieren und beheben Sie Kommunikationsprobleme 512

Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist 513

▼ So diagnostizieren Sie Probleme mit der PPP-Konfiguration 514

Allgemeine PPP-Konfigurationsprobleme 515

▼ So diagnostizieren Sie Modemprobleme 515

▼ So rufen Sie Informationen zur Fehlersuche für Chat-Skripten ab 516

Allgemeine Chat-Skript-Probleme 517

▼ So diagnostizieren und beheben Sie Probleme im Zusammenhang mit der Übertragungsrate einer seriellen Verbindung 519

▼ So rufen Sie Diagnoseinformationen für PPPoE ab 520

Beheben von Standleitungsproblemen 523

Diagnostizieren und Beheben von Authentifizierungsproblemen 523

22 Solaris PPP 4.0 (Referenz) 525
Verwenden von PPP-Optionen in Dateien und in der Befehlszeile 525
Wo PPP-Optionen definiert werden können 525
Wie PPP-Optionen verarbeitet werden 527
Funktionsweise der PPP-Konfigurationsdateiberechtigungen 528
`/etc/ppp/options`-Konfigurationsdatei 530
`/etc/ppp/options.` *ttyname*-Konfigurationsdatei 531
Konfigurieren von benutzerspezifischen Optionen 534
Konfigurieren von `$HOME/.pppprc` auf einem Einwahlserver 534
Konfigurieren von `$HOME/.pppprc` auf einem Hinauswahlrechner 534
Angeben von Informationen für die Kommunikation mit dem Einwahlserver 535
`/etc/ppp/peers/` *peer-name*-Datei 535
`/etc/ppp/peers/myisp.tmpl`-Vorlagendatei 536
Beispiele für die `/etc/ppp/peers/`*peer-name*-Dateien 537
Konfigurieren der Modemgeschwindigkeit für eine Wählverbindung 538
Definieren der Kommunikation über die Einwahlverbindung 538
Inhalt des Chat-Skripts 538
Beispiele für Chat-Skripten 539
Aufrufen des Chat-Skripts 546
▼ So rufen Sie ein Chat-Skript auf (Aufgabe) 547
Erstellen einer ausführbaren Chat-Datei 548
▼ So erstellen Sie ein ausführbares Chat-Programm 548
Authentifizieren von Anrufern 549
PAP (Password Authentication Protocol) 549
CHAP (Challenge-Handshake Authentication Protocol) 552
Erstellen eines IP-Adressierungsschemas für Anrufer 556
Zuweisen von dynamischen IP-Adressen für Anrufer 556
Zuweisen von statischen IP-Adressen für Anrufer 557
Zuweisen von IP-Adressen durch eine sppp-Einheitennummer 558
Erstellen von PPPoE-Tunneln für DSL-Unterstützung 558
Dateien zum Konfigurieren von Schnittstellen für PPPoE 559
Befehle und Dateien für den PPPoE-Zugangsserver 561
Befehle und Dateien für den PPPoE-Client 567

23 Migrieren von Asynchronous Solaris PPP zu Solaris PPP 4.0 (Aufgaben) 571
Vor dem Konvertieren von `asppp`-Dateien 571
Beispiel für eine `/etc/asppp.cf` -Konfigurationsdatei 572
Beispiel für die `/etc/uucp/Systems` -Datei 572
Beispiel für die `/etc/uucp/Devices` -Datei 573
Beispiel für die `/etc/uucp/Dialers` -Datei 573
Ausführen des `asppp2pppd`-Konvertierungsskripts (Aufgaben) 574
Voraussetzungen 574
▼ So konvertieren Sie von `asppp` in Solaris PPP 4.0 575
▼ So zeigen Sie die Ergebnisse der Konvertierung an 575

24 UUCP (Übersicht) 579
UUCP-Hardwarekonfigurationen 579
UUCP-Software 580
UUCP-Dämonen 580
UUCP-Verwaltungsprogramme 581
UUCP-Benutzerprogramme 582
UUCP-Datenbankdateien 583
Konfigurieren von UUCP-Datenbankdateien 584

25 Verwalten von UUCP (Aufgaben) 585
UUCP-Verwaltung (Übersicht der Schritte) 585
Hinzufügen von UUCP-Anmeldungen 586
▼ So fügen Sie UUCP-Anmeldungen hinzu 586
Starten von UUCP 587
▼ So starten Sie UUCP 588
`uudemon.poll`-Shell-Skript 588
`uudemon.hour`-Shell-Skript 588
`uudemon.admin`Shell-Skript 589
`uudemon.cleanup`-Shell-Skript 589
Ausführen von UUCP über TCP/IP 589
▼ So aktivieren Sie UUCP für TCP/IP 589
UUCP-Sicherheit und Verwaltung 590
Einrichten der UUCP-Sicherheit 590
Reguläre UUCP-Verwaltung 591

UUCP-Fehlerbehebung 592
▼ So stellen Sie fest, ob fehlerhafte Modems oder ACUs vorhanden sind 592
▼ So suchen Sie Übertragungsfehler 592
Prüfen der UUCP-/etc/uucp/Systems-Datei 594
Prüfen von UUCP-Fehlermeldungen 594
Prüfen von grundlegenden Informationen 595

26 UUCP (Referenz) 597
/etc/uucp/Systems-UUCP-Datei 597
Feld "System-Name" in der /etc/uucp/Systems-Datei 598
Feld "Time" in /etc/uucp/Systems-Datei 599
Feld "Type" in /etc/uucp/Systems-Datei 600
Feld "Speed" in /etc/uucp/Systems-Datei 600
Feld "Phone" in /etc/uucp/Systems-Datei 601
Feld "Chapt Script" in /etc/uucp/Systems-Datei 601
Aktivieren des Rückrufs durch das Chat-Skript 603
Hardware-Flusskontrolle in /etc/uucp/Systems -Datei 604
Einstellen der Parität in /etc/uucp/Systems-Datei 604
/etc/uucp/Devices-UUCP-Datei 605
Feld "Type" in /etc/uucp/Devices-Datei 606
Feld "Line" in /etc/uucp/Devices-Datei 607
Feld "Line2" in /etc/uucp/Devices-Datei 607
Feld "Class" in /etc/uucp/Devices-Datei 607
Feld "Dialer-Token-Pairs" in /etc/uucp/Devices-Datei 608
Struktur des Felds "Dialer-Token-Pairs" in /etc/uucp/Devices-Datei 609
Protokolldefinitionen in /etc/uucp/Devices-Datei 611
/etc/uucp/Dialers-UUCP-Datei 612
Aktivieren der Hardware-Flusskontrolle in /etc/uucp/Dialers -Datei 615
Einstellen der Parität in /etc/uucp/Dialers -Datei 616
Weitere grundlegende UUCP-Konfigurationsdateien 616
/etc/uucp/Dialcodes-UUCP-Datei 616
/etc/uucp/Sysfiles-UUCP-Datei 617
/etc/uucp/Sysname-UUCP-Datei 618
/etc/uucp/Permissions-UUCP-Datei 619
UUCP-Strukturierungseinträge 619

Überlegungen zu UUCP ... 620
REQUEST-UUCP-Option ... 620
SENDFILES-UUCP-Option ... 620
MYNAME-UUCP-Option ... 621
UUCP-READ- und -WRITE-Optionen ... 622
UUCP-NOREAD- und NOWRITE-Optionen ... 622
CALLBACK-UUCP-Option ... 623
COMMANDS-UUCP-Option ... 623
VALIDATE-UUCP-Option ... 625
UUCP- MACHINE-Eintrag für OTHER ... 626
Kombinieren der MACHINE- und LOGNAME-Einträge für UUCP ... 627
UUCP-Weiterleitung ... 627
UUCP- /etc/uucp/Poll-Datei ... 628
UUCP- /etc/uucp/Config-Datei ... 628
UUCP- /etc/uucp/Grades-Datei ... 628
UUCP-Feld "User-job-grade" ... 629
UUCP-Feld "System-job-grade" ... 629
UUCP-Feld "Job-size" ... 630
UUCP-Feld "Permit-type" ... 630
UUCP-Feld "ID-Liste" ... 631
Weitere UUCP-Konfigurationsdateien ... 631
/etc/uucp/Devconfig-UUCP-Datei ... 631
UUCP- /etc/uucp/Limits-Datei ... 632
UUCP- remote.unknown-Datei ... 632
UUCP-Verwaltungsdateien ... 633
UUCP-Fehlermeldungen ... 635
UUCP-ASSERT-Fehlermeldungen ... 635
UUCP-STATUS-Fehlermeldungen ... 636
Nummerische UUCP-Fehlermeldungen ... 638

Teil VI Arbeiten mit Remote-Systemen – Themen ... 641

27 Arbeiten mit Remote-Systemen (Übersicht) ... 643
Was ist ein FTP-Server? ... 643
Was ist ein Remote-System? ... 643

Aktuelle Änderungen am FTP-Service 644

28 Verwalten des FTP-Servers (Aufgaben) 647
Verwalten des FTP-Servers (Übersicht der Schritte) 647
Steuern des FTP-Serverzugriffs 649
▼ So definieren Sie FTP-Serverklassen 649
▼ So beschränken Sie Benutzeranmeldungen 650
▼ So legen Sie die Anzahl von ungültigen Anmeldeversuchen fest 652
▼ Wie bestimmten Benutzern der FTP-Serverzugriff verwehrt wird 653
▼ So beschränken Sie den Zugriff auf den standardmäßigen FTP-Server 654
Einrichten der Anmeldung für den FTP-Server 655
▼ So richten Sie den Zugriff für authentische FTP-Benutzer ein 656
▼ So richten Sie den Zugriff für FTP-Gastbenutzer ein 656
▼ So richten Sie den Zugriff für anonyme FTP-Benutzer ein 658
▼ So richten Sie die `/etc/shells`-Datei ein 658
Anpassen von Meldungsdateien 659
▼ So passen Sie Meldungsdateien an 659
▼ So erstellen Sie Meldungen, die an Benutzer gesendet werden 660
▼ So konfigurieren Sie die README-Option 661
Steuern des Zugriffs auf Dateien auf dem FTP-Server 663
▼ So steuern Sie Dateizugriffsbefehle 663
Steuern von Uploads und Downloads auf dem FTP-Server 664
▼ So steuern Sie Uploads auf den FTP-Server 664
▼ So steuern Sie Downloads auf den FTP-Server 666
Virtuelles Hosting 667
▼ So aktivieren Sie das limitierte virtuelle Hosting 668
▼ So aktivieren Sie komplettes virtuelles Hosting 669
Automatisches Starten des FTP-Servers 671
▼ So starten Sie einen FTP-Server mithilfe von SMF 671
▼ So starten Sie einen eigenständigen FTP-Server im Hintergrund 672
▼ So starten Sie einen eigenständigen FTP-Server im Vordergrund 673
Abschalten des FTP-Servers 673
▼ So schalten Sie den FTP-Server ab 673
Beheben von FTP-Serverproblemen 674
▼ So prüfen Sie `syslogd` auf FTP-Servermeldungen 675

▼ So verwenden Sie `greeting text`, um `ftpaccess` zu prüfen 675
▼ So stellen Sie fest, welche Befehle von FTP-Benutzern ausgeführt wurden 676
Konfigurationshilfe für Standorte mit hoher Auslastung 676

29 Zugriff auf Remote-Systeme (Aufgaben) 679
Zugriff auf Remote-Systeme (Übersicht der Schritte) 679
Anmelden bei einem Remote-System (`rlogin`) 680
Authentifizierung für Remote-Anmeldungen (`rlogin`) 680
Sequenzielle Remote-Anmeldungen 683
Direkte oder indirekte Remote-Anmeldungen 683
Vorgang nach der Remote-Anmeldung 684
▼ So gehen Sie vor, um nach `.rhosts`-Dateien zu suchen und diese zu entfernen 685
So stellen Sie fest, ob ein Remote-System funktioniert 686
So stellen Sie fest, wer bei einem Remote-System angemeldet ist 686
So melden Sie sich bei einem Remote-System an (`rlogin`) 687
So melden Sie sich bei einem Remote-System ab (`exit`) 688
Anmelden bei einem Remote-System (`ftp`) 688
Authentifizierung für Remote-Anmeldungen (`ftp`) 689
Wichtige `ftp`-Befehle 689
▼ So öffnen Sie eine `ftp`-Verbindung mit einem Remote-System 690
So schließen Sie eine `ftp`-Verbindung mit einem Remote-System 691
▼ So kopieren Sie Dateien aus einem Remote-System (`ftp`) 691
▼ So kopieren Sie Dateien in ein Remote-System (`ftp`) 693
Remote-Kopieren mit `rcp` 695
Sicherheitsüberlegungen für Kopiervorgänge 696
Angeben von Quelle und Ziel 696
▼ So kopieren Sie Dateien zwischen einem lokalen System und einem Remote-System (`rcp`) 698

Teil VII Überwachen von Netzwerkdiensten – Themen 701

30 Überwachen der Netzwerkleistung (Aufgaben) 703
Überwachen der Netzwerkleistung 703
So prüfen Sie die Antwort von Hosts im Netzwerk 704
So senden Sie Pakete an Hosts im Netzwerk 704

So erfassen Sie Pakete aus dem Netzwerk 705
So prüfen Sie den Netzwerkstatus 705
So zeigen Sie NFS-Server- und -Clientstatistiken an 708

Glossar 713

Index 719

Abbildungen

ABBILDUNG 2–1 Datenfluss beim NCA-Service 65
ABBILDUNG 6–1 Beziehung von RDMA zu anderen Protokollen 186
ABBILDUNG 6–2 Ansichten des Serverdateisystems und des Clientdateisystems 190
ABBILDUNG 6–3 Der `svc:/system/filesystem/autofs`-Service startet `automount`. 220
ABBILDUNG 6–4 Navigation durch die Master-Map 221
ABBILDUNG 6–5 Servernähe 225
ABBILDUNG 6–6 Wie autofs den Name Service verwendet 231
ABBILDUNG 7–1 Wichtige SLP-Agenten und Prozesse 239
ABBILDUNG 7–2 Implementierung von Agenten und Prozessen in der SLP-Architektur mit einem DA 239
ABBILDUNG 7–3 SLP-Implementierung 241
ABBILDUNG 12–1 Typische Konfiguration für die elektronische Übermittlung von Mails 297
ABBILDUNG 13–1 Lokale Mailkonfiguration 302
ABBILDUNG 13–2 Lokale Mailkonfiguration mit einer UUCP-Verbindung 303
ABBILDUNG 14–1 Gateway zwischen verschiedenen Kommunikationsprotokollen 366
ABBILDUNG 14–2 Interaktionen von Mailprogrammen 374
ABBILDUNG 15–1 Teile der PPP-Verbindung 425
ABBILDUNG 15–2 Einfache analoge PPP-Wählverbindung 427
ABBILDUNG 15–3 Standleitungskonfiguration 430
ABBILDUNG 15–4 Teilnehmer eines PPPoE-Tunnels 435
ABBILDUNG 16–1 Einwahlverbindung – Beispiel 441
ABBILDUNG 16–2 Beispiel einer Standleitungskonfiguration 444
ABBILDUNG 16–3 Beispiel eines PAP-Authentifizierungsszenarios (Heimarbeitsplatz) 447
ABBILDUNG 16–4 Beispiel eines CHAP-Authentifizierungsszenarios (Anwahl eines privaten Netzwerks) 449
ABBILDUNG 16–5 Beispiel eines PPPoE-Tunnels 453
ABBILDUNG 22–1 PAP-Authentifizierungsprozess 551
ABBILDUNG 22–2 Ablauf der CHAP-Authentifizierung 555

Tabellen

TABELLE 2–1 NCA-Dateien 63
TABELLE 3–1 NTP-Dateien 70
TABELLE 5–1 Übersicht der Schritte für gemeinsame Nutzung von Dateisystemen 87
TABELLE 5–2 Übersicht der Schritte für das Einhängen von Dateisystemen 90
TABELLE 5–3 Übersicht der Schritte für NFS-Services 96
TABELLE 5–4 Übersicht der Schritte für WebNFS-Systemverwaltungsaufgaben 104
TABELLE 5–5 Übersicht der Schritte für die Autofs-Verwaltung 107
TABELLE 5–6 Arten und Verwendung von autofs-Maps 110
TABELLE 5–7 Pflege von Maps 110
TABELLE 5–8 Wann der Befehl `automount` auszuführen ist 111
TABELLE 6–1 NFS-Dateien 141
TABELLE 6–2 Vordefinierte Map-Variablen 227
TABELLE 7–1 SLP-Agenten 238
TABELLE 9–1 SLP-Konfigurationsvorgänge 250
TABELLE 9–2 Eigenschaften zur zeitlichen Steuerung von DA-Advertisements und -Suchanforderungen 252
TABELLE 9–3 SLP-Leistungseigenschaften 257
TABELLE 9–4 Zeitüberschreitungseigenschaften 263
TABELLE 9–5 Konfigurieren mehrerer nicht gesteuerter Netzwerkschnittstellen 275
TABELLE 10–1 Beschreibung der SLP-Proxyregistrierungsdatei 284
TABELLE 11–1 SLP-Statuscodes 287
TABELLE 11–2 SLP-Meldungstypen 288
TABELLE 14–1 Allgemeine `sendmail`-Flags 352
TABELLE 14–2 Maps und Datenbanktypen 352
TABELLE 14–3 Betriebssystem-Flags 353
TABELLE 14–4 Nicht in dieser Version von `sendmail` verwendete generische Flags 353
TABELLE 14–5 Alternative `sendmail`-Befehle 354
TABELLE 14–6 Versionswerte für die Konfigurationsdatei 355
TABELLE 14–7 Domains der obersten Ebene 358

TABELLE 14–8 Konventionen für das Format von Mailbox-Namen 361
TABELLE 14–9 Für Mailservices verwendeter Inhalt des `/etc/mail/cf` -Verzeichnisses 370
TABELLE 14–10 Inhalt des `/usr/lib`-Verzeichnisses 372
TABELLE 14–11 Weitere Dateien, die für Mailservices verwendet werden 373
TABELLE 14–12 Spalten in der NIS+-Tabelle `mail_aliases` 382
TABELLE 14–13 Konfigurationsdateioptionen zum Ausführen von SMTP mit TLS 394
TABELLE 14–14 Makros zum Ausführen von SMTP mit TLS 396
TABELLE 14–15 Regellisten zum Ausführen von SMTP mit TLS 397
TABELLE 14–16 Befehlszeilenoptionen in Version 8.13 von `sendmail` 398
TABELLE 14–17 Konfigurationsdateioptionen in Version 8.13 von `sendmail` 398
TABELLE 14–18 `FEATURE()`-Deklarationen in Version 8.13 von `sendmail` 400
TABELLE 14–19 Zusätzliche oder eingestellte Befehlszeilenoptionen ab Version 8.12 von `sendmail` 403
TABELLE 14–20 Argumente für die Optionen `PidFile` und `ProcessTitlePrefix` 405
TABELLE 14–21 Zusätzliche definierte Makros für `sendmail` 405
TABELLE 14–22 Zusätzliche Makros zum Erstellen der `sendmail`-Konfigurationsdatei 406
TABELLE 14–23 Zusätzliche `MAX`-Makros 407
TABELLE 14–24 Zusätzliche und überarbeitete `m4`-Konfigurationsmakros für `sendmail` 408
TABELLE 14–25 Zusätzliche und überarbeitete `FEATURE()`-Deklarationen 409
TABELLE 14–26 Nicht unterstützte `FEATURE()`-Deklarationen 411
TABELLE 14–27 Zusätzliche Mailer-Flags 412
TABELLE 14–28 Zusätzliche Gleichsetzungen für Delivery Agents 413
TABELLE 14–29 Token-Vergleich 415
TABELLE 14–30 Zusätzliche LDAP-Map-Flags 415
TABELLE 14–31 Mögliche Werte für das erste Mailer-Argument 416
TABELLE 14–32 Neue Regellisten 416
TABELLE 16–1 Übersicht der Schritte für die PPP-Planung 438
TABELLE 16–2 Informationen für einen Hinauswahlrechner 439
TABELLE 16–3 Informationen für einen Einwahlserver 439
TABELLE 16–4 Planen einer Standleitungsverbindung 443
TABELLE 16–5 Voraussetzungen zum Konfigurieren der Authentifizierung 446
TABELLE 16–6 Planen der PPPoE-Clients 451
TABELLE 16–7 Planung für einen PPPoE-Zugangsserver 451
TABELLE 17–1 Übersicht der Schritte zum Einrichten der PPP-Wählverbindung 455
TABELLE 17–2 Übersicht der Schritte zum Einrichten des Hinauswahlrechners 456
TABELLE 17–3 Übersicht der Schritte zum Einrichten des Einwahlservers 464

TABELLE 18–1 Übersicht der Schritte zum Einrichten der Standleitungsverbindung 471
TABELLE 19–1 Übersicht der Schritte für die allgemeine PPP-Authentifizierung 478
TABELLE 19–2 Übersicht der Schritte für die PAP-Authentifizierung (Einwahlserver) 479
TABELLE 19–3 Übersicht der Schritte für die PAP-Authentifizierung (Hinauswahlrechner) . 479
TABELLE 19–4 Übersicht der Schritte für die CHAP-Authentifizierung (Einwahlserver) 487
TABELLE 19–5 Übersicht der Schritte für die CHAP-Authentifizierung (Hinauswahlrechner) 487
TABELLE 20–1 Übersicht der Schritte zum Einrichten eines PPPoE-Clients 495
TABELLE 20–2 Übersicht der Schritte zum Einrichten eines PPPoE-Zugangsservers 496
TABELLE 21–1 Übersicht der Schritte für die PPP-Fehlerbehebung 505
TABELLE 21–2 Allgemeine Netzwerkprobleme, von denen PPP betroffen ist 512
TABELLE 21–3 Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist 513
TABELLE 21–4 Allgemeine PPP-Konfigurationsprobleme 515
TABELLE 21–5 Allgemeine Chat-Skript-Probleme 517
TABELLE 21–6 Allgemeine Standleitungsprobleme 523
TABELLE 21–7 Allgemeine Authentifizierungsprobleme 524
TABELLE 22–1 Übersicht der PPP-Konfigurationsdateien und -Befehle 526
TABELLE 22–2 PPPoE-Befehle und -Konfigurationsdateien 559
TABELLE 25–1 Übersicht der Schritte für die UUCP-Verwaltung 585
TABELLE 26–1 Escape-Zeichen, die im Feld "Chat-Script" der `Systems` -Datei verwendet werden 602
TABELLE 26–2 Protokolle, die in `/etc/uucp/Devices` verwendet werden 611
TABELLE 26–3 Umgekehrter Schrägstrich für `/etc/uucp/Dialers` 614
TABELLE 26–4 Einträge in der `Dialcodes`-Datei 617
TABELLE 26–5 Feld "Permit-type" 631
TABELLE 26–6 UUCP-Sperrdateien 633
TABELLE 26–7 ASSERT-Fehlermeldungen 635
TABELLE 26–8 UUCP-STATUS-Meldungen 636
TABELLE 26–9 Nummerische UUCP-Fehlermeldungen 638
TABELLE 28–1 Übersicht der Schritte: Verwalten des FTP-Servers 647
TABELLE 29–1 Übersicht der Schritte: Zugriff auf Remote-Systeme 679
TABELLE 29–2 Abhängigkeiten zwischen Anmeldung und Authentifizierung (`rlogin`) 684
TABELLE 29–3 Wichtige `ftp`-Befehle 689
TABELLE 29–4 Zulässige Syntaxen für Verzeichnis- und Dateinamen 697
TABELLE 30–1 Befehle zur Überwachung des Netzwerks 703
TABELLE 30–2 Ausgabe des Befehls `netstat - r` 708

TABELLE 30–3 Befehle zum Anzeigen von Client- und Serverstatistiken 709
TABELLE 30–4 Ausgabe des Befehls `nfsstat -c` 710
TABELLE 30–5 Ausgabe des Befehls `nfsstat -m` 711

Beispiele

BEISPIEL 2–1 Verwenden eines Raw-Geräts als NCA-Protokolldatei 55
BEISPIEL 2–2 Verwenden mehrerer Dateien für die NCA-Protokollierung 55
BEISPIEL 2–3 Konfigurieren eines Apache 2.0-Webservers zur Verwendung des SSL-Kernel-Proxys 60
BEISPIEL 2–4 Konfigurieren eines Sun Java System-Webservers zur Verwendung eines SSL-Kernel-Proxys 62
BEISPIEL 2–5 Konfigurieren eines Apache-Webservers in einer lokalen Zone zur Verwendung eines SSL-Kernel-Proxys 62
BEISPIEL 3–1 Synchronisieren des Datums und der Uhrzeit mit einem anderen System 69
BEISPIEL 5–1 Eintrag in der `vfstab`-Datei des Clients 91
BEISPIEL 6–1 Aushängen eines Dateisystems 169
BEISPIEL 6–2 Verwenden von Optionen in Verbindung mit `umount` 170
BEISPIEL 6–3 `/etc/auto_master`-Beispieldatei 213
BEISPIEL 9–1 Einrichten von `slpd`, damit slpd als DA-Server fungieren kann 252
BEISPIEL 13–1 Einrichten der automatischen Neuerstellung der Datei `submit.cf` 316
BEISPIEL 13–2 `Received:` Mail-Header 322
BEISPIEL 13–3 Auflisten eines einzelnen Eintrags aus der NIS+-`mail_aliases`-Tabelle 326
BEISPIEL 13–4 Auflisten von teilweisen Entsprechungen aus der NIS+-`mail_aliases`-Tabelle 326
BEISPIEL 13–5 Löschen von Einträgen aus einer NIS+-`mail_aliases`-Tabelle 329
BEISPIEL 13–6 Ausgabe des Adressentestmodus 345
BEISPIEL 21–1 Ausgabe, die aus einer funktionierenden Wählverbindung resultiert 507
BEISPIEL 21–2 Ausgabe, die aus einer funktionierenden Standleitungsverbindung resultiert 508
BEISPIEL 22–1 Einzeiliges Chat-Skript 547
BEISPIEL 22–2 Grundlegende `/etc/ppp/pppoe`-Datei 563
BEISPIEL 22–3 `/etc/ppp/pppoe`-Datei für einen Zugangsserver 565
BEISPIEL 22–4 `/etc/ppp/options`-Datei für einen Zugangsserver 566
BEISPIEL 22–5 `/etc/hosts`-Datei für einen Zugangsserver 566
BEISPIEL 22–6 `/etc/ppp/pap-secrets`-Datei für einen Zugangsserver 566

BEISPIEL 22–7 `/etc/ppp/chap-secrets`-Datei für einen Zugangsserver 566
BEISPIEL 22–8 `/etc/ppp/peers/` *peer-name* zum Definieren eines Remote-Zugangsservers 568
BEISPIEL 26–1 Eintrag in `/etc/uucp/Systems` 598
BEISPIEL 26–2 Schlüsselwort für das Feld "Type" 600
BEISPIEL 26–3 Eintrag im Feld "Speed" 600
BEISPIEL 26–4 Eintrag im Feld "Phone" 601
BEISPIEL 26–5 Vergleich der Typfelder in der `Devices`-Datei und der `Systems` -Datei 607
BEISPIEL 26–6 Feld "Class" in `Devices`-Datei 608
BEISPIEL 26–7 Feld "Dialers" für ein direkt verbundenes Modem 609
BEISPIEL 26–8 UUCP-Feld "Dialers" für Computer am selben Portselektor 609
BEISPIEL 26–9 UUCP-Feld "dialer" für Modems, die mit einem Portselektor verbunden sind 610
BEISPIEL 26–10 Eintrag in `/etc/uucp/Dialers` -Datei 612
BEISPIEL 26–11 Auszüge aus `/etc/uucp/Dialers` 613
BEISPIEL 28–1 Definieren von FTP-Serverklassen 650
BEISPIEL 28–2 Beschränken von Benutzeranmeldungen 651
BEISPIEL 28–3 Festlegen der Anzahl von ungültigen Anmeldeversuchen 652
BEISPIEL 28–4 Verweigern des Zugriffs auf den FTP-Server 653
BEISPIEL 28–5 Beschränken des Zugriffs auf den standardmäßigen FTP-Server 655
BEISPIEL 28–6 Einrichten eines FTP-Servers für Gastbenutzer 657
BEISPIEL 28–7 Einrichten des Zugriffs für anonyme FTP-Benutzer 658
BEISPIEL 28–8 Erstellen der /etc/shells-Datei 658
BEISPIEL 28–9 Anpassen von Meldungsdateien 660
BEISPIEL 28–10 Erstellen von Meldungen, die an Benutzer gesendet werden 661
BEISPIEL 28–11 Konfigurieren der README-Option 662
BEISPIEL 28–12 Steuern von Dateizugriffsbefehlen 663
BEISPIEL 28–13 Steuern von Uploads auf den FTP-Server 665
BEISPIEL 28–14 Steuern von Downloads auf den FTP-Server 667
BEISPIEL 28–15 Aktivieren des limitierten virtuellen Hosting in der `ftpaccess`-Datei 669
BEISPIEL 28–16 Aktivieren des limitierten virtuellen Hosting über die Befehlszeile 669
BEISPIEL 28–17 Aktivieren des kompleten virtuellen Hosting in der `ftpservers`-Datei 670
BEISPIEL 28–18 Aktivieren des kompletten virtuellen Hosting über die Befehlszeile 670
BEISPIEL 29–1 Suchen nach `.rhosts`-Dateien und Entfernen dieser Dateien 685
BEISPIEL 29–2 Feststellen, wer bei einem Remote-System angemeldet ist 687
BEISPIEL 29–3 Anmelden bei einem Remote-System (`rlogin`) 688
BEISPIEL 29–4 Abmelden bei einem Remote-System (`exit`) 688

BEISPIEL 29–5 Öffnen einer `ftp`-Verbindung mit einem Remote-System 691
BEISPIEL 29–6 Kopieren von Dateien aus einem Remote-System (`ftp`) 692
BEISPIEL 29–7 Kopieren von Dateien in ein Remote-System (`ftp`) 694
BEISPIEL 29–8 Verwenden von `rcp`, um eine Remote-Datei auf ein lokales System zu kopieren 698
BEISPIEL 29–9 Verwenden von `rlogin` und `rcp`, um eine Remote-Datei in ein lokales System zu kopieren 699
BEISPIEL 29–10 Verwenden von `rcp`, um eine lokale Datei in ein Remote-System zu kopieren 699
BEISPIEL 29–11 Verwenden von `rlogin` und `rcp`, um eine lokale Datei auf ein Remote-System zu kopieren 699
BEISPIEL 30–1 Prüfen der Antwort von Hosts im Netzwerk 704
BEISPIEL 30–2 Senden von Paketen an Hosts im Netzwerk 705

Vorwort

Systemverwaltungshandbuch: Netzwerkdienste ist Teil eines mehrbändigen Dokumentationssets, in dem die wichtigsten Informationen zur Verwaltung des Betriebssystems Oracle Solaris beschrieben werden. In diesem Handbuch wird davon ausgegangen, dass das Betriebssystem Oracle Solaris 10 bereits installiert und eventuell erforderliche Netzwerksoftware eingerichtet ist.

Hinweis – Diese Oracle Solaris-Version unterstützt Systeme auf der Basis der Prozessorarchitekturen SPARC und x86. Die unterstützten Systeme finden Sie in den *Oracle Solaris OS: Hardware Compatibility Lists*. Eventuelle Implementierungsunterschiede zwischen den Plattformtypen sind in diesem Dokument angegeben.

In diesem Dokument bedeuten x86-bezogene Begriffe Folgendes:

- "x86" bezieht sich auf die große Familie der 64-Bit- und 32-Bit-kompatiblen x86-Produkte.
- "x64" bezieht sich insbesondere auf mit 64-Bit-x86-Architekturen kompatible CPUs.
- "32-Bit x86" weist auf spezifische, für 32-Bit-Systeme geltende Informationen zu x86-basierten Systemen hin.

Unterstützte Systeme finden Sie unter *Oracle Solaris OS: Hardware Compatibility Lists*.

Zielgruppe dieses Handbuchs

Dieses Handbuch richtet sich an Systemadministratoren, die für die Verwaltung von Systemen verantwortlich sind, auf denen das Betriebssystem Solaris 10 ausgeführt wird. Um die Informationen in diesem Handbuch richtig umsetzen zu können, sollten Sie über ein bis zwei Jahre Erfahrung in der Verwaltung von UNIX-Systemen verfügen. Die Teilnahme an Schulungen zur Verwaltung von UNIX-Systemen wird empfohlen.

Organisation der Systemverwaltungshandbücher

Hier finden Sie eine Liste der Themen, die in den Systemverwaltungshandbüchern behandelt werden.

Buchtitel	Themen
System Administration Guide: Basic Administration	Benutzerkonten und Gruppen, Server- und Clientunterstützung, Herunterfahren und Booten eines Systems, Verwalten der Services und Verwalten der Software (Pakete und Patches)
System Administration Guide: Advanced Administration	Terminale und Modems, Systemressourcen (Datenträgerkontingente, Accounting und Crontabs), Systemprozesse und Beheben von Problemen mit der Oracle Solaris-Software
System Administration Guide: Devices and File Systems	Wechselmedien, Festplatten und Geräte, Dateisysteme und Backup und Wiederherstellen von Daten
Systemverwaltungshandbuch: IP Services	TCP/IP-Netzwerkverwaltung, IPv4- und IPv6-Adressverwaltung, DHCP, IPsec, IKE, Solaris IP Filter, Mobile IP, IP-Netzwerk-Multipathing (IPMP) und IPQoS
Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)	DNS-, NIS- und LDAP-Naming Services und -Directory Services, einschließlich Übergang von NIS zu LDAP und Übergang von NIS+ zu LDAP
System Administration Guide: Naming and Directory Services (NIS+)	NIS+-Naming Services und Directory Services
Systemverwaltungshandbuch: Netzwerkdienste	Webcache-Server, zeitorientierte Services, Netzwerk-Dateisysteme (NFS und Autofs), Mail, SLP und PPP
System Administration Guide: Printing	Druckthemen und -aufgaben, wie Sie mithilfe von Services, Tools, Protokollen und Technologien Druckdienste und Drucker einrichten und verwalten
Systemverwaltungshandbuch: Sicherheitsservices	Auditing, Geräteverwaltung, Dateisicherheit, BART, Kerberos-Services, PAM, Solaris Cryptographic Framework, Berechtigungen, RBAC, SASL und Solaris Secure Shell
Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones	Projekte und Aufgaben im Rahmen der Ressourcenverwaltung, Extended Accounting, Resource Controls, Fair Share Scheduler (FSS), Steuerung des physischen Arbeitsspeichers mithilfe des Resource Capping Daemon (rcapd) und Resource Pools; Virtualisierung mithilfe der Softwarepartitionierungstechnologie Solaris Zones und `lx`-Branded Zones

Buchtitel	Themen
Oracle Solaris ZFS-Administrationshandbuch	ZFS-Speicherpool und Dateisystemerstellung und -verwaltung, Momentaufnahmen, Klone, Backups, verwenden von Zugriffssteuerlisten (Access Control Lists/ACLs) zum Schutz von ZFS-Dateien, verwenden von ZFS auf einem Oracle Solaris-System mit installierten Zonen, emulierte Datenträger und Problembehandlung und Datenwiederherstellung
Oracle Solaris Trusted Extensions Administrator's Procedures	Systemadministration, die nur für die Trusted Extensions-Funktion von Oracle Solaris gilt
Oracle Solaris Trusted Extensions Configuration Guide	Ab Version Solaris 10 5/08: Hier wird beschrieben, wie Sie die Trusted Extensions-Funktion von Oracle Solaris planen, aktivieren und die Erstkonfiguration durchführen.

Weiterführende Dokumentation

Auf die folgenden Dokumentationen wird in diesem Handbuch Bezug genommen:

- *System Administration Guide: Advanced Administration*
- *System Administration Guide: Basic Administration*
- *Systemverwaltungshandbuch: IP Services*
- *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*
- *System Administration Guide: Naming and Directory Services (NIS+)*
- *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*
- *Systemverwaltungshandbuch: Sicherheitsservices*
- Anderson, Bart, Bryan Costales und Harry Henderson. *UNIX Communications*. Howard W. Sams & Company, 1987.
- Costales, Bryan. *sendmail, Third Edition*. O'Reilly & Associates, Inc., 2002.
- Frey, Donnalyn und Rick Adams. *!%@:: A Directory of Electronic Mail Addressing and Networks*. O'Reilly & Associates, Inc., 1993.
- Krol, Ed. *The Whole Internet User's Guide and Catalog*. O' Reilly & Associates, Inc., 1993.
- O' Reilly, Tim und Grace Todino. *Managing UUCP and Usenet* . O' Reilly & Associates, Inc., 1992.

Weiterführende Informationen

Informationen zu PPPoE-Lizenzbedingungen finden Sie in den entsprechenden Dokumenten an folgenden Stellen:

/var/sadm/pkg/SUNWpppd/install/copyright

/var/sadm/pkg/SUNWpppdu/install/copyright

/var/sadm/pkg/SUNWpppg/install/copyright

Kontakt zum Support von Oracle

Oracle-Kunden können über My Oracle Support den Online-Support nutzen. Informationen dazu erhalten Sie unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` bzw. `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` (für Hörgeschädigte).

Typografische Konventionen

In der folgenden Tabelle sind die in diesem Handbuch verwendeten typografischen Konventionen aufgeführt.

TABELLE P–1 Typografische Konventionen

Schriftart	Bedeutung	Beispiel
`AaBbCc123`	Die Namen von Befehlen, Dateien, Verzeichnissen sowie Bildschirmausgabe.	Bearbeiten Sie Ihre `.login`-Datei. Verwenden Sie `ls -a`, um eine Liste aller Dateien zu erhalten. `system% Sie haben eine neue Nachricht.`
`AaBbCc123`	Von Ihnen eingegebene Zeichen (im Gegensatz zu auf dem Bildschirm angezeigten Zeichen)	`Computername%` **`su`** `Passwort:`
aabbcc123	Platzhalter: durch einen tatsächlichen Namen oder Wert zu ersetzen	Der Befehl zum Entfernen einer Datei lautet `rm` *Dateiname* .

TABELLE P–1 Typografische Konventionen *(Fortsetzung)*

Schriftart	Bedeutung	Beispiel
AaBbCc123	Buchtitel, neue Ausdrücke; hervorgehobene Begriffe	Lesen Sie hierzu Kapitel 6 im *Benutzerhandbuch*. Ein *Cache* ist eine lokal gespeicherte Kopie. Diese Datei *nicht* speichern. **Hinweis:** Einige hervorgehobene Begriffe werden online fett dargestellt.

Shell-Eingabeaufforderungen in Befehlsbeispielen

Die folgende Tabelle zeigt die UNIX-Standardeingabeaufforderung und die Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. Die in den Befehlsbeispielen angezeigte Standard-Systemeingabeaufforderung variiert, abhängig von der Oracle Solaris-Version.

TABELLE P–2 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	`$`
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	`#`
C-Shell	`system%`
C-Shell für Superuser	`system#`

TEIL I

Netzwerkdienste – Themen

Dieser Abschnitt enthält einen Überblick über das Handbuch, sowie eine Übersicht der Verfahren, aufgabenbezogene Informationen und Referenzinformationen zu NCA- und NTP-Services.

◆ ◆ ◆ KAPITEL 1

1 Netzwerkdienst (Übersicht)

Dieses Kapitel enthält eine Liste der Hauptthemen dieses Handbuchs. Außerdem ist eine Beschreibung des PERL-Service enthalten, der in dieser Solaris-Version enthalten ist.

- „Themen für Oracle Solaris 10 Update 10“ auf Seite 45
- „Perl 5“ auf Seite 46

Themen für Oracle Solaris 10 Update 10

In diesem Handbuch werden folgende Services oder Dienstprogramme behandelt:

„Perl 5“ auf Seite 46
: Perl (Practical Extraction and Report Language) ist ein Tool, das zum Generieren von Skripten verwendet werden kann, um die Erledigung von Systemverwaltungsaufgaben zu erleichtern.

Kapitel 2, „Verwalten von Webcache-Servern“
: NCA sorgt für eine verbesserte Webserverleistung, da Webseiten im Cache gespeichert werden.

Kapitel 3, „Zeitorientierte Services“
: NTP und zeitrelevante Dienstprogramme können verwendet werden, um die Zeit für viele Systeme zu synchronisieren.

Kapitel 4, „Verwalten von Netzwerkdateisystemen (Übersicht) “
: NFS ist ein Protokoll, das die Möglichkeit bietet, über einen Remote-Host auf Dateisysteme zuzugreifen.

Kapitel 7, „SLP (Übersicht)“
: SLP ist ein dynamisches Serviceerkennungsprotokoll.

Kapitel 12, „Mailservices (Übersicht)“
: Mailservices gestatten es, eine Nachricht an eine oder mehrere Personen zu senden, wenn die Nachricht über eines oder mehrere Netzwerke weitergeleitet werden muss.

Kapitel 15, „Solaris PPP 4.0 (Überblick)“
PPP ist ein Protokoll, das zur Bereitstellung von Point-to-Point-Verbindungen zwischen Remote-Hosts dient.

Kapitel 24, „UUCP (Übersicht)“
UUCP ermöglicht Hosts, Dateien auszutauschen.

Kapitel 27, „Arbeiten mit Remote-Systemen (Übersicht)“
Diese Befehle werden verwendet, um auf Dateien auf Remote-Systemen zuzugreifen. Zu diesen Befehlen zählen `ftp`, `rlogin` und `rcp`.

Perl 5

In dieser Solaris-Version ist Practical Extraction and Report Language (Perl) 5.8.4 enthalten, eine leistungsstarke, vielseitige Programmiersprache, die als kostenlose Software zur Verfügung steht. Perl hat sich aufgrund seiner ausgezeichneten Verarbeitungs-, Datei- und Textmanipulationsfunktionen als Standard-Entwicklungstool für komplexe Systemverwaltungsaufgaben etabliert.

Perl 5 bietet eine dynamisch ladbare modulare Grundstruktur, die es erlaubt, neue Funktionen für bestimmte Aufgaben zu integrieren. Viele Module sind kostenlos auf dem CPAN (Comprehensive Perl Archive Network) unter http://www.cpan.org erhältlich. Zum Erstellen und Installieren zusätzlicher Module von CPAN mithilfe von `gcc` können Sie das Skript `/usr/perl5/5.8.4/bin/perlgcc` verwenden. Weitere Informationen finden Sie auf der Manpage `perlgcc`(1).

Zugang zur Perl-Dokumentation

Diese Solaris-Version bietet verschiedene Quellen, denen Informationen zu Perl entnommen werden können. Diese Informationen erhalten Sie auch, wenn Sie wie folgt vorgehen:

Sie können auf die Manpages zugreifen, indem Sie `/usr/perl5/man` Ihrer MANPATH-Umgebungsvariable hinzufügen. Das folgende Beispiel dient zum Anzeigen der Perl-Übersicht:

```
% setenv MANPATH ${MANPATH}:/usr/perl5/man
% man perl
```

Sie können auf weitere Dokumentation zugreifen, indem Sie das Dienstprogramm `perldoc` verwenden. Im folgenden Beispiel werden diese Übersichtsinformationen angezeigt:

```
% /usr/perl5/bin/perldoc perl
```

Auf der `perl`-Übersichtsseite werden alle Dokumentationen aufgelistet, die in dieser Version enthalten sind.

Perl-Kompatibilitätsprobleme

Im Allgemeinen ist die Version 5.8.4 von Perl mit der Vorgängerversion kompatibel. Skripten müssen nicht neu erstellt oder neu kompiliert werden. XSUB-basierte (.xs) Module müssen jedoch neu kompiliert und neu installiert werden.

Änderungen an der Solaris-Version von Perl

Die Solaris-Version von Perl wurde kompiliert und unterstützt nun das Malloc-Verfahren, 64-Bit-Ganzzahlen und große Dateien. Außerdem wurden entsprechende Patches eingebracht. Eine vollständige Liste aller Konfigurationsinformationen können Sie in der Ausgabe des folgenden Befehls einsehen:

```
% /usr/perl5/bin/perlbug -dv
---
Flags:
    category=
    severity=
---
Site configuration information for perl v5.8.4:
 .
 .
```

Mithilfe von `perl -V` können Sie eine kürzere Liste ausgeben.

◆ ◆ ◆ KAPITEL 2

Verwalten von Webcache-Servern

Dieses Kapitel bietet einen Überblick über den NCA (Network Cache and Accelerator) von Solaris. Es sind außerdem Verfahren zur Verwendung des NCA sowie Referenzmaterial zu NCA enthalten. Des Weiteren sind für Solaris 10 6/06 eine Einführung zur Verwendung von SSL (Secure Sockets Layer) sowie Verfahren zur Verwendung des SSL-Kernel-Proxy zur Optimierung der SSL-Paketverarbeitung enthalten.

- „Network Cache and Accelerator (Übersicht) “ auf Seite 49
- „Verwalten von Webcache-Servern (Übersicht der Schritte)“ auf Seite 51
- „Verwalten der Zwischenspeicherung von Webseiten (Aufgaben)“ auf Seite 53
- „Zwischenspeicherung von Webseiten (Referenz)“ auf Seite 63

Network Cache and Accelerator (Übersicht)

Der NCA (Network Cache and Accelerator) von Solaris verbessert die Webserver-Leistung durch einen Kernel-Cache, der Webseiten enthält, auf die während der Verarbeitung von HTTP-Anforderungen zugegriffen wird. Dieser Kernel-Cache verwendet Systemspeicher, um die Leistung für HTTP-Anforderungen, die normalerweise von Webservern bearbeitet werden, wesentlich zu steigern. Durch die Verwendung eines Systemspeichers zur Aufbewahrung von Webseiten für HTTP-Anforderungen wird die Webserver-Leistung verbessert, da der Arbeitsaufwand zwischen dem Kernel und dem Webserver verringert wird. NCA stellt eine Sockets-Schnittstelle bereit, über die jeder Webserver mit NCA kommunizieren kann, wobei nur minimale Modifizierungen erforderlich sind.

Wenn eine angeforderte Seite aus dem Kernel-Cache abgerufen wird (Cachetreffer), ist die Leistungssteigerung besonders spürbar. Wenn sich die angeforderte Seite nicht im Cache befindet (Cachefehler) und vom Webserver abgerufen werden muss, ist die Leistung ebenfalls besser.

Dieses Produkt ist für einen dedizierten Webserver bestimmt. Wenn Sie auf einem Server, auf dem NCA ausgeführt wird, andere große Prozesse ausführen, können Probleme auftreten.

NCA bietet Protokollierungsunterstützung, indem Cachetreffer protokolliert werden. Dieses Protokoll wird im Binärformat gespeichert, um die Leistung zu erhöhen. Der Befehl `ncab2clf` kann verwendet werden, um dass Protokoll vom Binärformat in das CLF (Common Log Format) umzuwandeln.

Die Solaris-Version bietet folgende Erweiterungen:

- Sockets-Schnittstelle
- Unterstützung für sendfile mit Vektoren (unterstützt AF_NCA). Weitere Informationen finden Sie auf der Manpage `sendfilev(3EXT)`.
- Neue Optionen für den Befehl `ncab2clf`, mit dem Datensätze vor einem ausgewählten Datum (`-s`) übersprungen werden können und eine bestimmte Anzahl von Datensätzen (`-n`) verarbeitet werden kann
- `logd_path_name` in `ncalogd.conf` kann entweder ein Raw-Gerät, eine Datei oder eine Kombination aus beidem angeben.
- Unterstützung für einen Webserver zum Öffnen mehrerer AF_NCA-Sockets. Bei mehreren Sockets können Sie verschiedene Webserver einsetzen, die auf einem Server ausgeführt werden.
- Eine neue Konfigurationsdatei namens `/etc/nca/ncaport.conf`. Die Datei dient zum Verwalten von IP-Adressen und Ports, die von NCA verwendet werden. AF_NCA-Socket wird von Ihrem Webserver unter Umständen nicht standardmäßig unterstützt. Wenn Ihr Server diese Unterstützung nicht bietet, verwenden Sie diese Datei und die NCA-Socket-Dienstprogramm-Bibliothek, um einen AF_INET-Socket in einen AF_NCA-Socket umzuwandeln.

Webserver in Verbindung mit SSL-Protokoll (Secure Sockets Layer)

In Solaris 10 6/06 können ein Apache 2.0- und ein Sun Java System-Webserver so konfiguriert werden, dass das SSL-Protokoll verwendet werden kann. Das Protokoll sorgt für Vertraulichkeit, Nachrichtenintegrität und Endpunktauthentifizierung zwischen zwei Anwendungen. Der Kernel wurde geändert, um den SSL-Verkehr zu beschleunigen.

Der SSL-Kernel-Proxy implementiert die Serverseite des SSL-Protokolls. Der Proxy bietet eine bessere SSL-Leistung der Serveranwendungen (z. B. Webserver) gegenüber Anwendungen, die SSL-Bibliotheken auf Benutzerebene verwenden. Die Leistung kann je nach Arbeitsauslastung der Anwendung auf +35 % erhöht werden.

Der SSL-Kernel-Proxy unterstützt die SSL 3.0- und TLS 1.0-Protokolle sowie die meisten allgemein verwendeten Verschlüsselungspakete. Die vollständige Liste finden Sie auf der Manpage `ksslcfg(1M)`. Der Proxy kann so konfiguriert werden, dass er zum SSL-Server auf Benutzerebene zurückkehrt, wenn nicht unterstützte Verschlüsselungspakete vorhanden sind.

Am folgenden Verfahren wird aufgezeigt, wie Server konfiguriert werden müssen, damit der SSL-Kernel-Proxy verwendet werden kann:

- „So konfigurieren Sie einen Apache 2.0-Webserver, um den SSL-Kernel-Proxy zu verwenden“ auf Seite 58
- „So konfigurieren Sie einen Sun Java System-Webserver, um den SSL-Kernel-Proxy zu verwenden“ auf Seite 60
- „Verwenden des SSL-Kernel-Proxy in Zonen“ auf Seite 62

Verwalten von Webcache-Servern (Übersicht der Schritte)

In der folgenden Tabelle werden die Verfahren beschrieben, die zur Verwendung von NCA oder SSL benötigt werden.

Aufgabe	Beschreibung	Siehe
Planung für NCA	Probleme, die gelöst werden müssen, bevor Sie NCA aktivieren	„Planung für NCA“ auf Seite 52
Aktivieren von NCA	Schritte zum Aktivieren des Kernel-Caching von Webseiten auf einem Webserver	„So aktivieren Sie die Zwischenspeicherung von Webseiten“ auf Seite 53
Deaktivieren von NCA	Schritte zum Deaktivieren des Kernel-Caching von Webseiten auf einem Webserver	„So deaktivieren Sie die Zwischenspeicherung von Webseiten“ auf Seite 56
Verwalten der NCA-Protokollierung	Schritte zum Aktivieren oder Deaktivieren des NCA-Protokollierungsprozesses	„So aktivieren oder deaktivieren Sie die NCA-Protokollierung“ auf Seite 56
Laden der NCA-Socket-Bibliothek	Schritte zum Verwenden von NCA, wenn der AF_NCA-Socket nicht unterstützt wird	„So laden Sie die Socket-Dienstprogramm-Bibliothek für NCA“ auf Seite 57
Verwenden des SSL-Kernel-Proxy mit einem Apache 2.0-Webserver	Schritte zum Verwenden des SSL-Kernel-Proxy mit einem Webserver, um die SSL-Paketverarbeitung zu verbessern	„So konfigurieren Sie einen Apache 2.0-Webserver, um den SSL-Kernel-Proxy zu verwenden“ auf Seite 58
Verwenden des SSL-Kernel-Proxy mit einem Sun Java System-Webserver	Schritte zum Verwenden des SSL-Kernel-Proxy mit einem Webserver, um die SSL-Paketverarbeitung zu verbessern	„So konfigurieren Sie einen Sun Java System-Webserver, um den SSL-Kernel-Proxy zu verwenden“ auf Seite 60
Verwenden des SSL-Kernel-Proxy mit einem Webserver in einer lokalen Zone	Schritte zum Verwenden des SSL-Kernel-Proxy mit einem Webserver in einer lokalen Zone	„Verwenden des SSL-Kernel-Proxy in Zonen“ auf Seite 62

Planung für NCA

In den folgenden Abschnitten werden die Probleme behandelt, die vor dem Starten des NCA-Services gelöst werden müssen.

Systemanforderungen für NCA

Das System muss zur Unterstützung von NCA folgende Anforderungen erfüllen:

- RAM von 256 MB
- Solaris 10 bzw. 9 oder eine Solaris 8-Upgradeversion müssen installiert sein.
- Unterstützung für einen Webserver, der NCA standardmäßig unterstützt, oder ein Webserver, dessen Startskript zur Nutzung der Socket Utility Library für NCA modifiziert wurde:
  - Apache-Webserver (in Solaris 8-Upgrade, Solaris 9 und Oracle Solaris 10 enthalten)
  - Sun Java System-Webserver
  - Zeus-Webserver von Zeus Technology (`http://www.zeus.com`)

Dieses Produkt ist für einen dedizierten Webserver bestimmt. Wenn Sie auf einem Server, auf dem NCA ausgeführt wird, andere große Prozesse ausführen, können Probleme auftreten.

NCA-Protokollierung

Der NCA-Service kann konfiguriert werden, um Webaktivitäten zu protokollieren. Die NCA-Protokollierung sollte generell aktiviert sein, wenn die Webserver-Protokollierung aktiviert ist.

Interpositionsbibliothek für Dämon-Unterstützung des Tor-Servers

Viele Webserver verwenden AF_INET-Sockets. NCA verwendet standardmäßig AF_NCA-Sockets. Um dies zu korrigieren, wird eine Bibliothek zur Zwischenschaltung bereitgestellt. Die neue Bibliothek wird vor der standardmäßigen Socket-Bibliothek `libsocket.so` geladen. Der Bibliotheksaufruf `bind()` wird von der neuen Bibliothek `ncad_addr.so` zwischengeschaltet. Es wird davon ausgegangen, dass der Status in `/etc/nca/ncakmod.conf` aktiviert ist. Die Version von Apache, die in Solaris 9 und Solaris 10 enthalten ist, ist bereits für den Aufruf dieser Bibliothek konfiguriert. Wenn Sie IWS- oder Netscape-Server verwenden, informieren Sie sich unter „So laden Sie die Socket-Dienstprogramm-Bibliothek für NCA“ auf Seite 57, um die neue Bibliothek zu verwenden.

Unterstützung für mehrere Instanzen

Auf Systemen, auf denen NCA installiert ist, müssen oft mehrere Instanzen eines Webservers ausgeführt werden. Beispiel: Ein einzelner Server muss unter Umständen einen Webserver für den externen Zugriff sowie einen Verwaltungsserver unterstützen. Um diese Server zu trennen, richten Sie die Server so ein, dass sie jeweils einen separaten Port verwenden.

Verwalten der Zwischenspeicherung von Webseiten (Aufgaben)

In den folgenden Abschnitten werden die Verfahren beschrieben, um Teile des Services zu aktiviert oder zu deaktiviert.

▼ So aktivieren Sie die Zwischenspeicherung von Webseiten

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Registrieren Sie die Schnittstellen.

Tragen Sie den Namen jeder physischen Schnittstelle in die Datei `/etc/nca/nca.if` ein. Weitere Informationen finden Sie auf der Manpage `nca.if(4)`.

```
# cat /etc/nca/nca.if
hme0
hme1
```

Jede Schnittstelle muss über eine eigene `hostname.`*interface-name*-Datei und einen Eintrag in der `/etc/hosts`-Datei für den Inhalt von `hostname.`*interface-name* verfügen. Um die NCA-Funktion für alle Schnittstellen zu starten, fügen Sie ein Sternchen (`*`) in die Datei `nca.if` ein.

3 Aktivieren Sie das `ncakmod`-Kernel-Modul.

Ändern Sie den `status`-Eintrag in der Datei `/etc/nca/ncakmod.conf` in "aktiviert" (`enabled`).

```
# cat /etc/nca/ncakmod.conf
#
# NCA Kernel Module Configuration File
#
status=enabled
httpd_door_path=/var/run/nca_httpd_1.door
nca_active=disabled
```

Weitere Informationen finden Sie auf der Manpage `ncakmod.conf(4)`.

4 (Optional) Aktivieren Sie die NCA-Protokollierung.

Ändern Sie den `status`-Eintrag in der Datei `/etc/nca/ncalogd.conf` in "aktiviert" (`enabled`).

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

Sie können den Speicherort der Protokolldatei ändern, indem Sie den Pfad ändern, der durch den Eintrag `logd_path_name` angezeigt wird. Die Protokolldatei kann ein Raw-Gerät oder eine Datei sein. Die folgenden Beispiele stellen NCA-Protokolldateipfade dar. Weitere Informationen zur Konfigurationsdatei finden Sie auf der Manpage `ncalogd.conf(4)`.

5 (Optional) Definieren Sie Ports zur Unterstützung mehrerer Instanzen.

Tragen Sie die Portnummern in die Datei `/etc/nca/ncaport.conf` ein. Dieser Eintrag bewirkt, dass NCA bei allen konfigurierten IP-Adressen den Port 80 überwacht.

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
  .
  .
ncaport=*/80
```

6 Nur für x86: Vergrößern Sie den virtuellen Speicher.

Verwenden Sie den Befehl `eeprom`, um die `kernelbase` des Systems festzulegen.

```
# eeprom kernelbase=0x90000000
# eeprom kernelbase
kernelbase=0x90000000
```

Der zweite Befehl prüft, ob der Parameter gesetzt wurde.

Hinweis – Wenn Sie die `kernelbase` festlegen, verringern Sie die Größe des virtuellen Speichers, der für Benutzerprozesse verwendet werden kann, auf weniger als 3 GB. Durch diese Beschränkung ist das System nicht ABI-konform. Wenn das System gestartet wird, zeigt die Konsole eine Warnmeldung an, die auf Nichtkonformität hinweist. Für die meisten Programme ist kein virtueller Adressspeicher von 3 GB erforderlich. Wenn Sie ein Programm verwenden, das mehr als 3 GB benötigt, müssen Sie das Programm auf einem System ausführen, auf dem NCA nicht aktiviert ist.

---

7 Starten Sie den Server neu.

Beispiel 2–1 Verwenden eines Raw-Geräts als NCA-Protokolldatei

Die `logd_path_name`-Zeichenfolge in `ncalogd.conf` kann ein Raw-Gerät als Speicherplatz der NCA-Protokolldatei definieren. Der Vorteil eines Raw-Geräts besteht darin, dass der Service schneller ausgeführt werden kann, weil weniger Aufwand beim Zugreifen auf das Raw-Gerät entsteht.

Der NCA-Service testet jedes in der Datei aufgelistete Raw-Gerät, um sicherzustellen, dass kein Dateisystem vorhanden ist. Durch diesen Test wird gewährleistet, dass keine aktiven Dateisysteme versehentlich überschrieben werden.

Um zu verhindern, dass bei diesem Test ein Dateisystem gefunden wird, führen Sie den folgenden Befehl aus. Dieser Befehl zerstört einen Teil des Dateisystems auf jeder Festplattenpartition, die als Dateisystem konfiguriert war. In diesem Beispiel ist `/dev/rdsk/c0t0d0s7` das Raw-Gerät, auf dem sich ein altes Dateisystem befindet.

```
# dd if=/dev/zero of=/dev/rdsk/c0t0d0s7 bs=1024 count=1
```

Nachdem Sie `dd` ausgeführt haben, können Sie das Raw-Gerät in die Datei `ncalogd.conf` einfügen.

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/dev/rdsk/c0t0d0s7"
logd_file_size=1000000
```

Beispiel 2–2 Verwenden mehrerer Dateien für die NCA-Protokollierung

Die `logd_path_name`-Zeichenfolge in `ncalogd.conf` kann mehrere Ziele als Speicherplatz der NCA-Protokolldatei definieren. Die zweite Datei wird verwendet, wenn die erste Datei voll ist. Das folgende Beispiel zeigt, wie festgelegt wird, dass die `/var/nca/log`-Datei zunächst beschrieben und dann eine Rohpartition verwendet wird:

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log /dev/rdsk/c0t0d0s7"
logd_file_size=1000000
```

So deaktivieren Sie die Zwischenspeicherung von Webseiten

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Deaktivieren Sie das `ncakmod`-Kernel-Modul.**

Ändern Sie den `status`-Eintrag in der Datei `/etc/nca/ncakmod.conf` in `disabled`.

```
# cat /etc/nca/ncakmod.conf
# NCA Kernel Module Configuration File
#
status=disabled
httpd_door_path=/var/run/nca_httpd_1.door
nca_active=disabled
```

Weitere Informationen finden Sie auf der Manpage `ncakmod.conf(4)`.

3 **Deaktivieren Sie die NCA-Protokollierung.**

Ändern Sie den `status`-Eintrag in der Datei `/etc/nca/ncalogd.conf` in `disabled`.

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=disabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

Weitere Informationen finden Sie auf der Manpage `ncalogd.conf(4)`.

4 **Starten Sie den Server neu.**

So aktivieren oder deaktivieren Sie die NCA-Protokollierung

Die NCA-Protokollierung kann je nach Bedarf aktiviert oder deaktiviert werden, nachdem NCA aktiviert wurde. Weitere Informationen finden Sie unter „So aktivieren Sie die Zwischenspeicherung von Webseiten“ auf Seite 53.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Ändern Sie die NCA-Protokollierung.**

   Um die Protokollierung dauerhaft zu deaktivieren, müssen Sie den Status in der Datei `/etc/nca/ncalogd.conf` auf "deaktiviert" (`disabled`) setzen und das System neu starten. Weitere Informationen finden Sie auf der Manpage `ncalogd.conf(4)`.

   a. **Stoppen Sie die Protokollierung.**

      ```
      # /etc/init.d/ncalogd stop
      ```

   b. **Starten Sie die Protokollierung.**

      ```
      # /etc/init.d/ncalogd start
      ```

So laden Sie die Socket-Dienstprogramm-Bibliothek für NCA

Wenden Sie dieses Verfahren nur dann an, wenn Ihr Webserver das AF_NCA-Socket nicht standardmäßig unterstützt.

Fügen Sie in das Startskript des Webservers eine Zeile ein, die bewirkt, dass die Bibliothek vorgeladen wird. Diese Zeile sollte wie folgt aussehen:

```
LD_PRELOAD=/usr/lib/ncad_addr.so /usr/bin/httpd
```

▼ So fügen Sie einen neuen Port dem NCA-Service hinzu

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Fügen Sie einen neuen Port hinzu.**

   Fügen Sie einen neuen Porteintrag in die Datei `/etc/nca/ncaport.conf` ein. In diesem Beispiel wird Port `8888` für die IP-Adresse `192.168.84.71` eingefügt. Weitere Informationen finden Sie unter `ncaport.conf(4)`.

   ```
   # cat /etc/nca/ncaport.conf
   #
   # NCA Kernel Module Port Configuration File
   #
     .
     .
   ncaport=*/80
   ncaport=192.168.84.71/8888
   ```

3 **Starten Sie eine neue Webinstanz.**

In der Datei, in der die NCA-Portkonfigurationen enthalten sind, muss eine Adresse vorhanden sein, bevor ein Webserver die Adresse für NCA verwenden kann. Wenn der Webserver ausgeführt wird, muss er neu gestartet werden, nachdem die neue Adresse definiert wurde.

▼ So konfigurieren Sie einen Apache 2.0-Webserver, um den SSL-Kernel-Proxy zu verwenden

Dieses Verfahren dient zur Verbesserung der Leistung des SSL-Paketprozesses, der auf einem Apache 2.0-Webserver ausgeführt wird.

Bevor Sie beginnen

Für das folgende Verfahren muss ein Apache 2.0-Webserver installiert und konfiguriert sein. Der Apache 2.0-Webserver ist in enthalten.

Um den SSL-Kernel-Proxy verwenden zu können, müssen der private Serverschlüssel und das Serverzertifikat in einer einzelnen Datei enthalten sein. Wenn nur der Parameter `SSLCertificateFile` in der Datei `ssl.conf` angegeben ist, kann die angegebene Datei direkt für Kernel-SSL verwendet werden. Wenn der Parameter `SSLCertificateKeyFile` ebenfalls angegeben ist, müssen die Zertifikatsdatei und die Privatschlüsseldatei kombiniert werden. Eine Möglichkeit, das Zertifikat und die Schlüsseldatei zu kombinieren, besteht darin, den folgenden Befehl auszuführen:

```
# cat cert.pem key.pem >cert-and-key.pem
```

1 **Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*. Der Befehl `ksslcfg` ist im `Network Security`-Profil enthalten.

2 **Stoppen Sie den Webserver.**

Dieser Befehl stoppt den Webserver auf einem System, auf dem der Server so konfiguriert ist, dass er mithilfe von SMF ausgeführt wird.

```
# svcadm disable svc:/network/http:apache2
```

Wenn der Service noch nicht umgewandelt wurde, stoppen Sie den Service mit der Befehlssyntax `/usr/apache2/bin/apachectl stop`.

3 **Legen Sie mithilfe des Befehls `ksslcfg` fest, welche Parameter verwendet werden sollen.**

Sämtliche Optionen finden Sie auf der Manpage `ksslcfg(1M)`. Sie müssen über Informationen für die folgenden Parameter verfügen:

- `key-format` – wird zusammen mit der Option `-f` verwendet, um das Zertifikat und das Schlüsselformat zu definieren. Für den SSL-Kernel-Proxy sollte entweder `pem` oder `pkcs12` verwendet werden.
- `key-and-certificate-file` – wird zusammen mit der Option `-i` verwendet, um den Speicherort der Datei festzulegen, in der der Serverschlüssel und das Zertifikat gespeichert werden.
- `password-file` – wird zusammen mit der Option `-p` verwendet, um den Speicherort der Datei festzulegen, in der das Passwort gespeichert wird, das zum Verschlüsseln des privaten Schlüssels dient. Dieses Passwort wird verwendet, um unbeaufsichtigte Neustarts zu erlauben. Die Berechtigungen für die Datei sollten auf `0400` gesetzt sein.
- `proxy-port` – wird zusammen mit der Option `-x` verwendet, um den SSL-Proxyport festzulegen. Wählen Sie einen anderen Port als den Standardport `80`. Der Webserver überwacht den SSL-Proxyport.
- `ssl-port` – dient zur Auswahl des Ports für den SSL-Kernel-Proxy, der überwacht werden soll. Der Wert wird normalerweise auf `443` gesetzt.

Hinweis – Die Werte für `ssl-port` und `proxy-port` können nicht für NCA konfiguriert werden, da diese Ports ausschließlich vom SSL-Kernel-Proxy verwendet werden. Normalerweise wird Port 80 für NCA, Port 8443 für den `Proxy-Port` und Port 443 für den `SSL-Port` verwendet.

---

4 Erstellen Sie die Serviceinstanz.

Der Befehl `ksslcfg` gibt den SSL-Proxyport und die zugehörige Parameter an.

`ksslcfg create -f` *key-format* `-i` *key-and-certificate-file* `-p` *password-file* `-x` *proxy-port ssl-port*

5 Stellen Sie sicher, dass die Instanz ordnungsgemäß erstellt wurde.

Der Servicestatus, der durch den folgenden Befehl gemeldet wird, sollte "online" lauten:

```
# svcs svc:/network/ssl/proxy
```

6 Konfigurieren Sie den Webserver so, dass dieser den SSL-Proxyport überwacht.

Bearbeiten Sie die Datei `/etc/apache2/http.conf`, und fügen Sie eine Zeile ein, um den SSL-Proxyport zu definieren. Wenn Sie die Server-IP-Adresse verwenden, überwacht der Webserver nur die betreffende Schnittstelle. Die Zeile sollte wie folgt aussehen:

`Listen 0.0.0.0:`*proxy-port*

7 Legen Sie eine SMF-Abhängigkeit für den Webserver fest.

Der Webserver sollte nur nach der SSL-Kernel-Proxyinstanz gestartet werden. Die folgenden Befehle dienen zum Festlegen dieser Abhängigkeit:

```
# svccfg -s svc:/network/http:apache2
svc:/network/http:apache2> addpg kssl dependency
```

```
svc:/network/http:apache2> setprop kssl/entities = fmri:svc:/network/ssl/proxy:kssl-INADDR_ANY-443
svc:/network/http:apache2> setprop kssl/grouping = astring: require_all
svc:/network/http:apache2> setprop kssl/restart_on = astring: refresh
svc:/network/http:apache2> setprop kssl/type = astring: service
svc:/network/http:apache2> end
```

8 Aktivieren Sie den Webserver.

```
# svcadm enable svc:/network/http:apache2
```

Wenn der Service nicht mithilfe von SMF gestartet wird, verwenden Sie den folgenden Befehl: `/usr/apache2/bin/apachectl startssl`

Beispiel 2–3 Konfigurieren eines Apache 2.0-Webservers zur Verwendung des SSL-Kernel-Proxys

Der folgende Befehl erstellt eine Instanz mithilfe des `pem`-Schlüsselformats:

```
# ksslcfg create -f pem -i cert-and-key.pem -p file -x 8443 443
```

▼ So konfigurieren Sie einen Sun Java System-Webserver, um den SSL-Kernel-Proxy zu verwenden

Dieses Verfahren dient zur Verbesserung der Leistung des SSL-Paketprozesses, der auf einem Sun Java System-Webserver ausgeführt wird. Informationen zu diesem Webserver finden Sie im *Sun Java System Web Server 6.1 SP4 Administrator's Guide* .

Bevor Sie beginnen Für das folgende Verfahren muss ein Sun Java System-Webserver installiert und konfiguriert sein.

1 Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*. Der Befehl `ksslcfg` ist im `Network Security`-Profil enthalten.

2 Stoppen Sie den Webserver.

Verwenden Sie die Administrator-Webschnittstelle, um den Server zu stoppen. Weitere Informationen finden Sie unter *Starting and Stopping the Server* im *Sun Java System Web Server 6.1 SP4 Administrator's Guide* .

3 Deaktivieren Sie den Metaslot der Verschlüsselungsstruktur.

Dieser Schritt ist notwendig, um sicherzustellen, dass der Metaslot deaktiviert ist, wenn die Instanz des Kernel-SSL-Service erstellt wird.

```
# cryptoadm disable metaslot
```

4 Legen Sie mithilfe des Befehls `ksslcfg` fest, welche Parameter verwendet werden sollen.

Sämtliche Optionen finden Sie auf der Manpage `ksslcfg(1M)`. Sie müssen über Informationen für die folgenden Parameter verfügen:

- `key-format` – wird zusammen mit der Option `-f` verwendet, um das Zertifikat und das Schlüsselformat zu definieren.
- `token-label` – wird zusammen mit der Option `-T` verwendet, um das PKCS#11-Token anzugeben.
- `certificate-label` – wird zusammen mit der Option `-C` verwendet, um die Bezeichnung im Zertifikatobjekt im PKCS#11-Token auszuwählen.
- `password-file` – wird zusammen mit der Option `-p` verwendet, um den Speicherort der Datei festzulegen, die das Passwort enthält, das verwendet wird, um den Benutzer beim PKCS#11-Token anzumelden, das vom Webserver verwendet wird. Dieses Passwort wird verwendet, um unbeaufsichtigte Neustarts zu erlauben. Die Berechtigungen für die Datei sollten auf `0400` gesetzt sein.
- `proxy-port` – wird zusammen mit der Option `-x` verwendet, um den SSL-Proxyport festzulegen. Wählen Sie einen anderen Port als den Standardport `80`. Der Webserver überwacht den SSL-Proxyport.
- `ssl-port` – definiert den Port für den SSL-Kernel-Proxy, der überwacht werden soll. Dieser Wert wird normalerweise auf `443` gesetzt.

Hinweis – Die Werte für `ssl-port` und `proxy-port` können nicht für NCA konfiguriert werden, da diese Ports ausschließlich vom SSL-Kernel-Proxy verwendet werden. Normalerweise wird Port 80 für NCA, Port 8443 für den `Proxy-Port` und Port 443 für den `SSL-Port` verwendet.

---

5 Erstellen Sie die Serviceinstanz.

Der Befehl `ksslcfg` gibt den SSL-Proxyport und die zugehörige Parameter an.

```
ksslcfg create -f key-format -T PKCS#11-token -C certificate-label -p password-file -x proxy-port ssl-port
```

6 Aktivieren Sie den Metaslot der Verschlüsselungsstruktur.

```
# cryptoadm enable metaslot
```

7 Stellen Sie sicher, dass die Instanz ordnungsgemäß erstellt wurde.

Der Servicestatus, der durch den folgenden Befehl gemeldet wird, sollte "online" lauten:

```
# svcs svc:/network/ssl/proxy
```

8. **Konfigurieren Sie den Webserver so, dass dieser den SSL-Proxyport überwacht.**

   Weitere Informationen finden Sie unter *Adding and Editing Listen Sockets* im *Sun Java System Web Server 6.1 SP4 Administrator's Guide* .

9. **Starten Sie den Webserver.**

Beispiel 2–4 Konfigurieren eines Sun Java System-Webservers zur Verwendung eines SSL-Kernel-Proxys

Der folgende Befehl erstellt eine Instanz mithilfe des `pkcs11`-Schlüsselformats:

```
# ksslcfg create -f pkcs11 -T "Sun Software PKCS#11 softtoken" -C "Server-Cert" -p file -x 8443 443
```

Verwenden des SSL-Kernel-Proxy in Zonen

Die Verwendung des SSL-Kernel-Proxy in Zonen unterliegt folgenden Beschränkungen:

- Die gesamte Kernel-SSL-Verwaltung muss von der globalen Zone aus durchgeführt werden. Der Administrator der globalen Zone benötigt Zugriff auf das Zertifikat der lokalen Zone sowie die Schlüsseldateien. Der Webserver der lokalen Zone kann gestartet werden, sobald die Serviceinstanz mithilfe des Befehls `ksslcfg` in der globalen Zone konfiguriert ist.
- Es muss ein spezifischer Hostname oder eine IP-Adresse angegeben werden, wenn der Befehl `ksslcfg` ausgeführt wird, um die Instanz zu konfigurieren. Die Instanz kann vor allem INADDR_ANY nicht verwenden.

BEISPIEL 2–5 Konfigurieren eines Apache-Webservers in einer lokalen Zone zur Verwendung eines SSL-Kernel-Proxys

Stoppen Sie in der lokalen Zone zunächst den Webserver. Führen Sie in der lokalen Zone alle Schritte aus, die notwendig sind, um den Service zu konfigurieren. Um eine Instanz namens `apache-zone` für eine lokale Zone zu erstellen, verwenden Sie den folgenden Befehl:

```
# ksslcfg create -f pem -i /zone/apache-zone/root/keypair.pem -p /zone/apache-zone/root/pass \
    -x 8443 apache-zone 443
```

Führen Sie in der lokalen Zone den folgenden Befehl aus, um die Serviceinstanz zu aktivieren:

```
# svcadm enable svc:/network/http:apache2
```

Zwischenspeicherung von Webseiten (Referenz)

In den folgenden Abschnitten wird auf die Dateien und Komponenten eingegangen, die zur Verwendung von NCA benötigt werden. Auch wird beschrieben, wie NCA mit dem Webserver interagiert.

NCA-Dateien

Sie benötigen mehrere Dateien, um die NCA-Funktion zu unterstützen. Viele dieser Dateien sind ASCII-Dateien, aber einige sind binäre Dateien. In der nachstehenden Tabelle werden alle Dateien aufgelistet.

TABELLE 2–1 NCA-Dateien

Dateiname	Funktion
`/dev/nca`	Der Pfadname für das NCA-Gerät
`/etc/hostname.*`	Eine Datei, die alle physischen Schnittstellen auflistet, die auf dem Server konfiguriert sind
`/etc/hosts`	Eine Datei, die alle Hostnamen auflistet, die dem Server zugeordnet sind. Die Einträge in dieser Datei müssen mit den Einträgen in den `/etc/hostname.*` -Dateien übereinstimmen, damit NCA funktioniert.
`/etc/init.d/ncakmod`	Das Skript, das den NCA-Server startet. Dieses Skript wird ausgeführt, wenn ein Server neu gestartet wird.
`/etc/init.d/ncalogd`	Das Skript, das die NCA-Protokollierung startet. Dieses Skript wird ausgeführt, wenn ein Server neu gestartet wird.
`/etc/nca/nca.if`	Eine Datei, die die Schnittstellen auflistet, über die NCA ausgeführt wird. Weitere Informationen finden Sie auf der Manpage `nca.if(4)`.
`/etc/nca/ncakmod.conf`	Eine Datei, die die Konfigurationsparameter für NCA auflistet. Weitere Informationen finden Sie auf der Manpage `ncakmod.conf(4)`.
`/etc/nca/ncalogd.conf`	Eine Datei, die die Konfigurationsparameter für die NCA-Protokollierung auflistet. Weitere Informationen finden Sie auf der Manpage `ncalogd.conf(4)`.
`/etc/nca/ncaport.conf`	Eine Datei, die die IP-Adressen und die Ports für NCA auflistet. Weitere Informationen finden Sie auf der Manpage `ncaport.conf(4)`.

TABELLE 2–1 NCA-Dateien *(Fortsetzung)*

Dateiname	Funktion
`/usr/bin/ncab2clf`	Ein Befehl, der verwendet wird, um Daten in der Protokolldatei in ein allgemeines Protokollformat zu konvertieren. Weitere Informationen finden Sie auf der Manpage `ncab2clf(1)`.
`/usr/lib/net/ncaconfd`	Ein Befehl, der verwendet wird, um NCA zu konfigurieren, damit NCA während des Startvorgangs über mehrere Schnittstellen ausgeführt wird. Weitere Informationen finden Sie auf der Manpage `ncaconfd(1M)`.
`/usr/lib/nca_addr.so`	Eine Bibliothek, die AF_NCA-Sockets anstelle von AF_INET-Sockets verwendet. Diese Bibliothek muss für Webserver verwendet werden, die AF_INET-Sockets verwenden. Weitere Informationen finden Sie auf der Manpage `ncad_addr(4)`.
`/var/nca/log`	Datei, in der Protokolldateidaten enthalten sind. Diese Datei sollte nicht bearbeitet werden, da sie ein binäres Format hat.
`/var/run/nca_httpd_1.door`	Der Name des Torpfads

NCA-Architektur

Die NCA-Funktion weist folgende Komponenten auf:

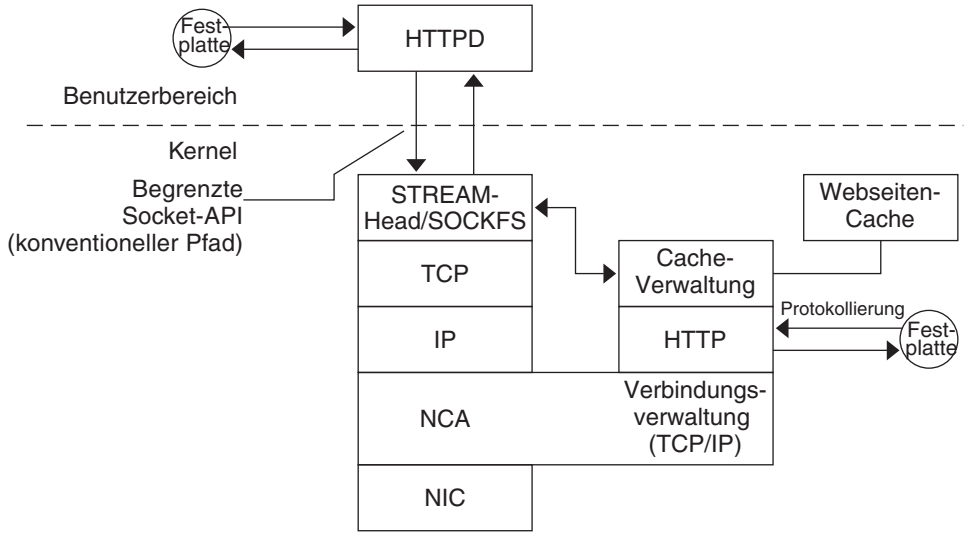
- Kernel-Modul, `ncakmod`
- Webserver, `httpd`

Das Kernel-Modul `ncakmod` verwaltet den Cache der Webseiten im Systemspeicher. Das Modul kommuniziert mit einem Webserver, `httpd` , über eine Sockets-Schnittstelle. Der Familientyp ist PF_NCA.

Das Kernel-Modul stellt auch eine Protokollierungsfunktion bereit, die alle HTTP-Cachetreffer protokolliert. Bei der NCA-Protokollierung werden HTTP-Daten im Binärformat auf die Festplatte geschrieben. NCA bietet ein Konvertierungsdienstprogramm zum Konvertieren von binären Protokolldateien in ein CLF-Format.

In der folgenden Abbildung wird der Datenfluss des herkömmlichen Pfads und des Pfads gezeigt, der verwendet wird, wenn NCA aktiviert ist.

ABBILDUNG 2–1 Datenfluss beim NCA-Service



Datenfluss von NCA zu Httpd, der aus einer Anforderung resultiert

In der folgenden Liste wird der aus einer Anforderung resultierende Datenfluss zwischen dem Client und dem Webserver beschrieben.

1. Eine HTTP-Anforderung wird vom Client an den Webserver gesendet.
2. Wenn die Seite im Cache gespeichert ist, wird die im Kernel-Cache gespeicherte Webseite zurückgegeben.
3. Wenn sich die Seite nicht im Cache befindet, wird die Anforderung an den Webserver weitergegeben, wodurch die Seite abgerufen oder aktualisiert wird.
4. Von der Semantik des HTTP-Protokolls, die in der Antwort verwendet wird, hängt ab, ob die Seite im Cache gespeichert wird oder nicht. Anschließend wird die Seite an den Client zurückgegeben. Wenn die Kopfzeile "Pragma: No-cach" in der HTTP-Anforderung enthalten ist, wird die Seite nicht im Cache gespeichert.

◆ ◆ ◆ KAPITEL 3

Zeitorientierte Services

Für viele Datenbanken und Authentifizierungsservices ist es erforderlich, das die Systemuhren innerhalb eines Netzwerks stets synchronisiert sind. In diesem Kapitel werden folgende Themen behandelt.

- „Uhrsynchronisierung (Übersicht)“ auf Seite 67
- „Verwalten von Network Time Protocol (Aufgaben)“ auf Seite 68
- „Verwenden anderer zeitorientierter Befehle (Aufgaben)“ auf Seite 69
- „Network Time Protocol (Referenz)“ auf Seite 70

Uhrsynchronisierung (Übersicht)

In der Solaris-Software ist die allgemein zugängliche NTP-Software (Network Time Protocol) der University of Delaware integriert. Der `xntpd`-Dämon dient zur Einstellung und Kontrolle der Systemuhrzeit. Der `xntpd`-Dämon ist eine vollständige Implementierung des Standards der Version 3, der durch das RFC 1305 definiert ist.

Der `xntpd`-Dämon liest die `/etc/inet/ntp.conf`-Datei während des Systemstarts. Weitere Informationen zu Konfigurationsoptionen finden Sie auf der Manpage `xntpd(1M)`.

Beim Einsatz von NPT in Ihrem Netzwerk ist Folgendes zu beachten:

- Der `xntpd`-Dämon verwendet minimale Systemressourcen.
- Ein NTP-Client wird automatisch mit einem NTP-Server synchronisiert, wenn er gebootet wird. Wenn die Synchronisierung des Clients nicht mehr gegeben ist, wird der Client erneut synchronisiert, sobald er einen Zeitserver kontaktiert.

Eine andere Möglichkeit der Synchronisierung von Uhren besteht darin, `rdate` auszuführen, während `cron` verwendet wird.

Verwalten von Network Time Protocol (Aufgaben)

Das folgende Verfahren zeigt, wie der NTP-Service eingerichtet und verwendet wird.

▼ So richten Sie einen NTP-Server ein

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erstellen Sie die `ntp.conf`-Datei.**

   Um sicherzustellen, dass der `xntpd`-Dämon richtig ausgeführt wird, muss zunächst die `ntp.conf`-Datei erstellt werden. Die `ntp.server`-Datei kann als Vorlage verwendet werden.

   ```
   # cd /etc/inet
   # cp ntp.server ntp.conf
   ```

3. **Starten Sie den `xntpd`-Dämon.**

   ```
   # svcadm enable network/ntp
   ```

▼ So richten Sie einen NTP-Client ein

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erstellen Sie die `ntp.conf`-Datei.**

   Um den `xntpd`-Dämon zu aktivieren, muss zunächst die `ntp.conf`-Datei erstellt werden.

   ```
   # cd /etc/inet
   # cp ntp.client ntp.conf
   ```

3. **Starten Sie den `xntpd`-Dämon.**

   ```
   # svcadm enable network/ntp
   ```

Verwenden anderer zeitorientierter Befehle (Aufgaben)

Wenden Sie das folgende Verfahren an, um die aktuelle Zeit jederzeit nach Bedarf zu aktualisieren, ohne NTP einrichten zu müssen.

▼ So synchronisieren Sie Datum und Uhrzeit mit einem anderen System

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Synchronisieren Sie das Datum und die Uhrzeit mit einem anderen System, indem Sie den Befehl `rdate` verwenden.**

```
# rdate another-system
```

another-system Name des anderen Systems

3 **Stellen Sie sicher, dass Sie das Datum Ihres Systems mithilfe des Befehls `date` zurückgesetzt haben.**

Die Ausgabe sollte ein Datum und eine Uhrzeit enthalten, die mit dem Datum und der Uhrzeit des anderen Systems übereinstimmen.

Beispiel 3–1 Synchronisieren des Datums und der Uhrzeit mit einem anderen System

Das folgende Beispiel zeigt, wie `rdate` zu verwenden ist, um das Datum und die Uhrzeit eines Systems mit dem Datum und der Uhrzeit eines anderen Systems zu synchronisieren. In diesem Beispiel wird das System `earth`, das mehrere Stunden nachgeht, zurückgestellt, damit es mit dem Datum und der Uhrzeit des Servers `starbug` übereinstimmt.

```
earth# date
Tue Jun  5 11:08:27 MDT 2001
earth# rdate starbug
Tue Jun  5 14:06:37 2001
earth# date
Tue Jun  5 14:06:40 MDT 2001
```

Network Time Protocol (Referenz)

Die folgenden Dateien werden benötigt, damit der NTP-Service ausgeführt werden kann.

TABELLE 3–1 NTP-Dateien

Dateiname	Funktion
`/etc/inet/ntp.conf`	Listet Konfigurationsoptionen für NTP auf.
`/etc/inet/ntp.client`	Beispielkonfigurationsdatei für NTP-Clients
`/etc/inet/ntp.server`	Beispielkonfigurationsdatei für NTP-Server
`/etc/inet/ntp.keys`	Enthält NTP-Berechtigungsschlüssel.
`/usr/lib/inet/xntpd`	NTP-Dämon. Weitere Informationen finden Sie auf der Manpage `xntpd`(1M).
`/usr/sbin/ntpdate`	Dienstprogramm zum Festlegen des lokalen Datums und der Uhrzeit auf der Basis von NTP. Weitere Informationen finden Sie auf der Manpage `ntpdate`(1M).
`/usr/sbin/ntpq`	NTP-Abfrageprogramm. Weitere Informationen finden Sie auf der Manpage `ntpq`(1M).
`/usr/sbin/ntptrace`	Programm, das dazu dient, NTP-Hosts bis zum NTP-Master-Server zurückzuverfolgen. Weitere Informationen finden Sie auf der Manpage `ntptrace`(1M).
`/usr/sbin/xntpdc`	NTP-Abfrageprogramm für den `xntpd`-Dämon. Weitere Informationen finden Sie auf der Manpage `xntpdc`(1M).
`/var/ntp/ntpstats`	Verzeichnis für NTP-Statistiken
`/var/ntp/ntp.drift`	Legt den anfänglichen Frequenzversatz für NTP-Server fest.

TEIL II

Zugriff auf Netzwerkdateisysteme – Themen

Dieser Abschnitt enthält eine Übersicht sowie aufgabenbezogene und Referenzinformationen zum Thema NFS-Services.

◆ ◆ ◆ KAPITEL 4

Verwalten von Netzwerkdateisystemen (Übersicht)

Dieses Kapitel bietet eine Übersicht über den NFS-Service, der verwendet werden kann, um über das Netzwerk auf Dateisysteme zuzugreifen. Außerdem werden in diesem Kapitel Konzepte zum Verständnis des NFS-Service sowie neueste Funktionen von NFS und autofs erläutert.

- „Neue Funktionen des NFS-Service“ auf Seite 73
- „NFS-Terminologie“ auf Seite 75
- „Informationen zum NFS-Service“ auf Seite 76
- „Informationen zu Autofs“ auf Seite 77
- „Funktionen des NFS-Service“ auf Seite 77

Hinweis – Wenn auf Ihrem System aktivierte Zonen vorhanden sind und Sie beabsichtigen, diese Funktion in einer nicht globalen Zone zu verwenden, lesen Sie *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*, um weitere Informationen zu erhalten.

Neue Funktionen des NFS-Service

Dieser Abschnitt enthält Informationen zu neuen Funktionen in verschiedenen Solaris-Versionen.

Änderungen in Solaris 10 11/06

Solaris 10 11/06 bietet Unterstützung für das Dateisystemüberwachungstool. Folgende Informationen stehen zur Verfügung:

- Eine Beschreibung und Beispiele unter „`fsstat`-Befehl“ auf Seite 162
- Weitere Informationen auf der Manpage `fsstat`(1M)

Außerdem enthält dieses Handbuch eine ausführliche Beschreibung des Dämons `nfsmapid`. Informationen zu `nfsmapid` finden Sie hier:

- „`nfsmapid`-Dämon“ auf Seite 151
- Manpage `nfsmapid`(1M)

Eine vollständige Liste der neuen Funktionen finden Sie unter *Neuerungen in Oracle Solaris 10 8/11*.

Änderungen in Solaris 10

Ab Solaris 10 ist die NFS-Version 4 die Standardversion. Informationen zu den Funktionen in NFS-Version 4 und anderen Änderungen finden Sie unter:

- „Version 4 des NFS-Protokolls“ auf Seite 78
- „`/etc/default/autofs`-Datei“ auf Seite 143
- „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144
- „`lockd`-Dämon“ auf Seite 148
- „`nfs4cbd`-Dämon“ auf Seite 149
- „`nfsmapid`-Dämon“ auf Seite 151
- „`mount`-Optionen für NFS-Dateisysteme“ auf Seite 163
- „NFS über RDMA“ auf Seite 185
- „Versionsaushandlung in NFS“ auf Seite 187
- „Funktionen in NFS-Version 4“ auf Seite 188
- „Wie autofs die nächsten schreibgeschützten Dateien für Clients auswählt (mehrere Speicherorte)“ auf Seite 223

Außerdem stehen folgende Informationen zur Verfügung:

- Aufgabenbezogene Informationen unter „Einrichten von NFS-Services“ auf Seite 96
- Eine vollständige Liste der neuen Funktionen finden Sie unter *Neuerungen in Oracle Solaris 10 8/11*.

Außerdem wird der NFS-Service von der Service Management Facility verwaltet. Administrative Maßnahmen an diesem Service, beispielsweise Aktivieren, Deaktivieren oder Neustarten, können mithilfe des Befehls `svcadm` vorgenommen werden. Der Status des Service kann mit dem Befehl `svcs` abgefragt werden. Weitere Informationen zur Service Management Facility finden Sie auf der Manpage `smf`(5) und in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*.

NFS-Terminologie

Dieser Abschnitt beschreibt grundlegende Termini, mit denen Sie sich vertraut machen sollten, um mit dem NFS-Service arbeiten zu können. Weiterführende Informationen zum NFS-Service finden Sie in Kapitel 6, „Zugreifen auf Netzwerkdateisysteme (Referenz) “.

NFS-Server und -Clients

Die Begriffe *Client* und *Server* werden verwendet, um die Rollen eines Computeres bei der Freigabe von Dateisystemen zu beschreiben. Computer, deren gemeinsam genutzte Dateisysteme in einem Netzwerk zur Verfügung stehen, fungieren als Server. Computer, die auf Dateisysteme zugreifen, werden als Clients bezeichnet. Der NFS-Service ermöglicht jedem Computer, auf die Dateisysteme anderer Computer zuzugreifen. Gleichzeitig bietet der NFS-Service Zugriff auf seine eigenen Dateisysteme. Ein Computer kann jederzeit die Rolle eines Clients oder Servers oder die Rolle eines Clients und eines Servers in einem Netzwerk annehmen.

Clients greifen auf die Dateien eines Servers zu, indem die gemeinsam genutzten Dateisysteme des Servers eingehängt werden. Wenn ein Client ein Remote-Dateisystem einhängt, wird keine Kopie des Dateisystems erstellt. Stattdessen erfolgen im Einhängungsprozess eine Reihe von Remote-Prozeduraufrufen, die dem Client ermöglichen, transparent auf das Dateisystem auf der Festplatte des Servers zuzugreifen. Die Einhängung ist einer lokalen Einhängung ähnlich. Die Benutzer können Befehle wie bei einem lokalen Dateisystem eingeben. Aufgabenbezogene Informationen zum Einhängen von Dateisystemen finden Sie unter „Einhängen von Dateisystemen“ auf Seite 90.

Nachdem ein Dateisystem über NFS auf einem Server zur gemeinsamen Nutzung freigegeben wurde, kann über einen Client auf das Dateisystem zugegriffen werden. Sie können ein NFS-Dateisystem automatisch mit autofs einhängen. Unter „Automatische Freigabe von Dateisystemen“ auf Seite 86 und „Aufgabenübersicht für die Autofs-Verwaltung“ auf Seite 107 finden Sie aufgabenbezogene Informationen zum Befehl `share` und autofs.

NFS-Dateisysteme

Zu den Objekten, die mit dem NFS-Service zur gemeinsamen Nutzung freigegeben werden können, zählen eine komplette oder teilweise Verzeichnisstruktur oder eine Dateihierarchie sowie einzelne Dateien. Ein Computer kann keine Dateihierarchie gemeinsam nutzen, die eine bereits gemeinsam genutzte Dateihierarchie überlagert. Peripheriegeräte wie Modems und Drucker können nicht gemeinsam genutzt werden.

In den meisten UNIX-Systemumgebungen stimmt der Aufbau einer Dateihierarchie, die gemeinsam genutzt werden kann, mit dem Aufbau eines Dateisystems oder eines Teils eines Dateisystems überein. Jedoch ist die NFS-Unterstützung betriebssystemübergreifend, und das

Konzept eines Dateisystems ist in anderen Nicht-UNIX-Umgebungen möglicherweise bedeutungslos. Aus diesem Grund bezieht sich der Begriff *Dateisystem* auf eine Datei oder eine Dateihierarchie, die gemeinsam genutzt und mit NFS eingehängt werden kann.

Informationen zum NFS-Service

Der NFS-Service ermöglicht Computern mit unterschiedlichen Architekturen, auf denen verschiedene Betriebssysteme ausgeführt werden, auf gemeinsam genutzte Dateisysteme in einem Netzwerk zuzugreifen. Die NFS-Unterstützung wurde auf vielen Plattformen implementiert, darunter MS-DOS- und VMS-Betriebssysteme.

Die NFS-Umgebung kann auf verschiedenen Betriebssystemen implementiert werden, da NFS ein abstraktes Modell eines Dateisystems definiert, aber keine architektonische Spezifikation. Jedes Betriebssystem verwendet das NFS-Modell für seine Dateisystemsemantik. Bei einem solchen Modell funktionieren Dateisystemvorgänge (z. B. Lesen und Schreiben) so, als ob auf eine lokale Datei zugegriffen wird.

Der NFS-Service bietet folgende Vorteile:

- Zugriff mehrerer Computer auf dieselben Dateien, wodurch Zugriff auf dieselben Daten im Netzwerk möglich ist
- Senkung von Speicherkosten durch gemeinsame Nutzung von Anwendungen, sodass kein lokaler Festplattenspeicher für einzelne Benutzeranwendungen bereitgestellt werden muss
- Datenkonsistenz und Zuverlässigkeit, da alle Benutzer Zugriff auf dieselben Daten haben
- Transparenz der Einhängung von Dateisystemen für Benutzer
- Transparenz des Zugriffs auf Remote-Dateien für Benutzer
- Unterstützung heterogener Umgebungen
- Senkung des Systemverwaltungsaufwands

Beim NFS-Service ist der physische Speicherort eines Dateisystems für den Benutzer irrelevant. Sie können die NFS-Implementierung verwenden, um Benutzern zu ermöglichen, sämtliche relevanten Dateien anzuzeigen, egal wo diese sich befinden. Anstatt häufig verwendete Dateien auf jedes System zu kopieren, können Sie dank des NFS-Services, eine einzige Kopie auf der Festplatte des Computers speichern. Alle anderen Systeme greifen über das Netzwerk auf die Dateien zu. Mit NFS sind Remote-Dateisysteme fast nicht mehr von lokalen Dateisystemen zu unterscheiden.

Informationen zu Autofs

Dateisysteme, die mit dem NFS-Service zur gemeinsamen Nutzung freigegeben werden, können mithilfe der automatischen Einhängung eingehängt werden. Autofs, ein Clientservice, ist eine Dateisystemstruktur, die das automatische Einhängen ermöglicht. Das autofs-Dateisystem wird vom Dämon `automount` initialisiert, der automatisch ausgeführt wird, wenn ein System neu gestartet wird. Der automount-Dämon, `automountd`, wird ständig ausgeführt und hängt Remote-Verzeichnisse nach Bedarf ein und aus.

Wenn ein Clientcomputer, auf dem `automountd` ausgeführt wird, versucht, auf eine Remote-Datei oder ein Remote-Verzeichnis zuzugreifen, hängt der Dämon das Remote-Dateisystem ein. Das Remote-Dateisystem bleibt eingehängt, solange dies nötig ist. Wird für eine bestimmte Zeit nicht auf das Remote-Dateisystem zugegriffen, wird es automatisch ausgehängt.

Das Einhängen muss nicht während des Boot-Vorgangs ausgeführt werden, und der Benutzer muss nicht mehr das Superuser-Passwort kennen, um ein Verzeichnis einzuhängen. Benutzer müssen nicht die Befehle `mount` und `umount` verwenden. Der autofs-Service hängt Dateisysteme nach Bedarf ein und aus, ohne dass ein Eingreifen des Benutzers nötig ist.

Das Einhängen mancher Dateihierarchien mit `automountd` schließt nicht die Möglichkeit des Einhängens anderer Hierarchien mit `mount` aus. Ein Computer ohne lokalen Massenspeicher *muss* `/` (root), `/usr` und `/usr/kvm` mithilfe des Befehls `mount` und der `/etc/vfstab`-Datei einhängen.

Ausführliche Informationen zum autofs-Service finden Sie unter „Aufgabenübersicht für die Autofs-Verwaltung“ auf Seite 107 und „Funktionsweise von autofs“ auf Seite 219.

Funktionen des NFS-Service

In diesem Abschnitt werden die wichtigsten Funktionen des NFS-Service beschrieben.

Version 2 des NFS-Protokolls

Version 2 war die erste weitverbreitete Version des NFS-Protokolls. Version 2 steht weiterhin auf zahlreichen Plattformen zur Verfügung. Alle Solaris-Versionen unterstützen Version 2 des NFS-Protokolls. Die Vorgängerversionen von Solaris 2.5 unterstützen jedoch nur Version 2.

Version 3 des NFS-Protokolls

Die Implementierung der Version 3 des NFS-Protokolls war eine Neuheit in Solaris 2.5. Verschiedene Änderungen wurden implementiert, um die Interoperabilität und Leistung zu verbessern. Die Protokollversion 3 muss sowohl auf den NFS-Servern als auch auf den NFS-Clients ausgeführt werden, damit optimale Ergebnisse erzielt werden.

Anders als bei der Version 2 des NFS-Protokolls besitzt Version 3 die Fähigkeit, Dateien zu verarbeiten, die größer als 2 GB sind. Die vorherige Beschränkung wurde entfernt. Lesen Sie dazu „NFS-Unterstützung für große Dateien“ auf Seite 81.

Die Version 3 des NFS-Protokolls ermöglicht sichere asynchrone Schreibvorgänge auf dem Server, wodurch die Leistung verbessert wird, da der Server clientseitige Schreibanforderungen zwischenspeichern kann. Der Client muss nicht warten, bis der Server die Änderungen auf der Festplatte bestätigt, wodurch die Reaktionszeit verkürzt wird. Zudem kann der Server die Anforderungen bündeln, wodurch ebenfalls zur Kürzung der Reaktionszeit auf dem Server beigetragen wird.

Bei vielen Vorgängen der NFS-Version 3 von Solaris werden Dateiattribute zurückgegeben, die im lokalen Cache gespeichert werden. Da der Cache häufig aktualisiert wird, ist es weniger oft nötig, die betreffenden Daten separat zu aktualisieren. Dementsprechend wird die Anzahl der RPC-Aufrufe an den Server verringert, wodurch die Leistung verbessert wird.

Der Vorgang zur Prüfung von Dateizugriffsberechtigungen wurde verbessert. In Version 2 wurde eine Schreib- oder Lesefehlermeldung ausgegeben, wenn ein Benutzer versuchte, eine Remote-Datei ohne die entsprechenden Berechtigungen zu kopieren. In Version 3 werden die Berechtigungen vor dem Öffnen einer Datei geprüft. Wenn dabei ein Fehler auftritt, wird die Meldung "Fehler beim Öffnen" ausgegeben.

In Version 3 des NFS-Protokolls wurde die Beschränkung der 8-KB-Übertragungsgröße entfernt. Die Übertragungsgröße kann zwischen Clients und Servern ausgehandelt werden, wodurch die 8-KB-Beschränkung der Version 2 bedeutungslos ist. In Solaris 2.5 ist für das Protokoll standardmäßig eine Übertragungsgröße von 32 KB definiert. Ab Solaris 10 wurden die Beschränkungen der leitungsgebundenen Übertragungsgrößen gelockert. Die Übertragungsgröße basiert nun auf den Funktionen des zugrunde liegenden Transportmechanismus.

Version 4 des NFS-Protokolls

Die NFS-Version 4 bietet Funktionen, die nicht in den Vorgängerversionen enthalten sind.

In Version 4 des NFS-Protokolls werden die Benutzer-ID und die Gruppen-ID als Zeichenfolge dargestellt. `nfsmapid` wird vom Client und vom Server für Folgendes verwendet:

- Zuordnen der ID-Zeichenfolgen von Version 4 zu einer lokalen numerischen ID
- Zuordnen der lokalen numerischen IDs zu ID-Zeichenfolgen von Version 4

Weitere Informationen finden Sie unter „`nfsmapid`-Dämon“ auf Seite 151.

Bitte beachten Sie: In der NFS-Version 4 wird der ID-Mapper `nfsmapid` verwendet, um Benutzer- oder Gruppen-IDs in Zugriffssteuerungslisteneinträgen auf einem Server den Benutzer- oder Gruppen-IDs in Zugriffssteuerungslisteneinträgen auf einem Client zuzuordnen. Die Zuordnung erfolgt auch in umgekehrter Richtung. Weitere Informationen finden Sie unter „Zugriffskontrolllisten (ACLs) und `nfsmapid` in NFS-Version 4“ auf Seite 197.

Wenn Sie mit NFS-Version 4 die gemeinsame Nutzung eines Dateisystems aufheben, werden sämtliche Zustände von geöffneten Dateien oder Dateisperrungen im betreffenden Dateisystem außer Kraft gesetzt. In NFS-Version 3 wurden von Clients veranlasste Sperrungen vom Server beibehalten, bevor die gemeinsame Nutzung des Dateisystems aufgehoben wurde. Weitere Informationen finden Sie unter „Aufheben der gemeinsamen Nutzung und erneutes Freigeben zur gemeinsamen Nutzung eines Dateisystems in NFS-Version 4“ auf Seite 188.

Die Server der NFS-Version 4 verwenden ein Pseudodateisystem, das Clients den Zugriff auf exportierte Objekte auf einem Server ermöglicht. In den Vorgängerversionen war kein Pseudodateisystem vorhanden. Weitere Informationen finden Sie unter „Dateisystem-Namespace in NFS-Version 4“ auf Seite 189.

In den NFS-Versionen 2 und 3 wurden vom Server dauerhafte Dateizugriffsroutinen zurückgegeben. NFS-Version 4 unterstützt temporäre Dateizugriffsroutinen. Weitere Informationen finden Sie unter „Temporäre Dateizugriffsroutinen in NFS-Version 4“ auf Seite 191.

Delegierung, ein Verfahren, bei dem ein Server die Verwaltung einer Datei an einen Client delegiert, wird sowohl für Clients als auch Server unterstützt. Ein Server kann beispielsweise einem Client eine Lese- oder Schreibdelegierung gewähren. Weitere Informationen finden Sie unter „Delegierung in NFS-Version 4“ auf Seite 195.

Ab Solaris 10 bietet die NFS-Version 4 keine Unterstützung für die LIPKEY/SPKM-Sicherheitsvariante.

Außerdem werden folgende Dämonen nicht verwendet:

- `mountd`
- `nfslogd`
- `statd`

Eine vollständige Liste der Funktionen von NFS-Version 4 finden Sie unter „Funktionen in NFS-Version 4“ auf Seite 188.

Verfahrensbezogene Informationen zur Verwendung der NFS-Version 4 finden Sie unter „Einrichten von NFS-Services“ auf Seite 96.

Steuerung von NFS-Versionen

Die `/etc/default/nfs`-Datei weist Schlüsselwörter auf, die zum Steuern der NFS-Protokolle dienen, die vom Client und vom Server verwendet werden. Die Versionsaushandlung kann beispielsweise mithilfe von Schlüsselwörtern gesteuert werden. Weitere Informationen finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144 oder auf der Manpage `nfs(4)`.

NFS-ACL-Unterstützung

In Solaris 2.5 wurde die Unterstützung der Zugriffskontrollliste (ACL) implementiert. Zugriffskontrolllisten ermöglichen eine feinere Abstimmung der Festlegung von Dateizugriffsberechtigungen als bei standardmäßigen UNIX-Dateiberechtigungen. Durch die NFS-ACL-Unterstützung ist es möglich, von einem Solaris-NFS-Client aus Zugriffskontrolllisteneinträge auf einem Solaris-NFS-Server zu ändern und anzuzeigen.

Die Protokolle der NFS-Versionen 2 und 3 unterstützen die alten POSIX-basierten Zugriffskontrolllisten. POSIX-basierte Zugriffskontrolllisten werden von UFS unterstützt. Weitere Informationen zu UFS-ACLs finden Sie unter „Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Das Protokoll der NFS-Version 4 unterstützt die neuen NFSv4-basierten Zugriffssteuerungslisten. NFSv4-basierte Zugriffssteuerungslisten werden von ZFS unterstützt. Um sämtliche Funktionen von NFSv4-basierten Zugriffssteuerungslisten nutzen zu können, muss ZFS als zugrunde liegendes Dateisystem auf dem NFSv4-Server verwendet werden. Neben den standardmäßigen Lese-, Schreib- und Ausführungsberechtigungen besitzen NFSv4-basierte Zugriffssteuerungslisten zahlreiche herkömmliche Eigenschaften sowie eine Reihe von Berechtigungsbits. Eine Übersicht der neuen Zugriffssteuerungslisten finden Sie in Kapitel 8, „Schützen von Oracle Solaris ZFS-Dateien mit Zugriffssteuerungslisten und Attributen“ in *Oracle Solaris ZFS-Administrationshandbuch*. Weitere Informationen zur Unterstützung für Zugriffssteuerungslisten in NFS-Version 4 finden Sie unter „Zugriffskontrolllisten (ACLs) und `nfsmapid` in NFS-Version 4“ auf Seite 197.

NFS über TCP

Das Standardtransportprotokoll für das NFS-Protokoll wird in Solaris 2.5 durch das TCP (Transport Control Protocol) ersetzt. TCP verbessert die Leistung in langsamen Netzwerken und Weitverkehrsnetzwerken (WAN). Außerdem bietet TCP Funktionen zur Steuerung bei Überlastung und zur Wiederherstellung nach Fehlern. NFS über TCP lässt sich kombinieren mit Version 2, 3 und 4. Vor Solaris 2.5 wurde anstelle des standardmäßigen NFS-Protokolls das UDP (User Datagram Protocol) verwendet.

NFS über UDP

Ab Solaris 10 verwendet der NFS-Client wesentlich weniger UDP-Ports. Zuvor belegten NFS-Übertragungen über UDP für jede ausstehende Anforderung einen separaten UDP-Port. Jetzt verwendet der NFS-Client standardmäßig nur noch einen reservierten UDP-Port. Diese Unterstützung ist jedoch konfigurierbar. Wenn die Bereitstellung mehrerer gleichzeitiger Ports die Systemleistung durch eine erhöhte Skalierbarkeit verbessern würde, kann das System so konfiguriert werden, dass es auf mehrere Ports zugreift. Damit ist dieselbe Konfigurierbarkeit erreicht, die für die Unterstützung vor NFS-über-TCP seit ihrer Einführung vorhanden war. Weitere Informationen finden Sie im *Oracle Solaris Tunable Parameters Reference Manual* .

Hinweis – UDP wird in NFS-Version 4 nicht verwendet. Wenn Sie ein Dateisystem mit der Option `proto=udp` einhängen, wird die NFS-Version 3 anstelle der Version 4 verwendet.

Übersicht zu NFS über RDMA

Solaris 10 enthält ein RDMA-Protokoll (Remote Direct Memory Access). Hierbei handelt es sich um ein Verfahren zur Übertragung von Daten zwischen Speichern über Hochgeschwindigkeitsnetzwerke. RDMA sorgt vor allem für die direkte Remote-Datenübertragung zwischen Speichern ohne Eingreifen der CPU. Dies ist möglich, weil RDMA die E/A-Verbindungstechnologie der InfiniBand-on-SPARC-Plattformen mit den Funktionen des Betriebssystems Solaris vereint. Weitere Informationen finden Sie unter „NFS über RDMA“ auf Seite 185.

Netzwerk-Sperren-Manager und NFS

Solaris 2.5 enthält zudem eine verbesserte Version des Netzwerk-Sperren-Managers. Der Netzwerk-Sperren-Manager wurde zum Sperren von UNIX-Datensätzen und für die gemeinsame PC-Nutzung für NFS-Dateien verwendet. Die Zuverlässigkeit des Sperrmechanismus für NFS-Dateien wurde verbessert, wodurch Sperrbefehle nun weniger fehleranfällig sind.

Hinweis – Der Netzwerk-Sperren-Manager wird nur in NFS-Versionen 2 und 3 für Einhängungen verwendet. Die Dateisperrung ist in das Protokoll der NFS-Version 4 integriert.

NFS-Unterstützung für große Dateien

Die Implementierung von Solaris 2.6 des Protokolls der NFS-Version 3 wurde geändert, damit Dateien bearbeitet werden können, die größer als 2 GB sind. Mit dem Protokoll der NFS-Version 2 und der Implementierung von Solaris 2.5 der Protokollversion 3 war es nicht möglich, Dateien zu bearbeiten, die größer als 2 GB sind.

NFS-Client-Failover

In Solaris 2.6 wurde dynamisches Failover von schreibgeschützten Systemen implementiert. Das Failover sorgt für eine hohe Verfügbarkeit schreibgeschützter Ressourcen, die bereits repliziert sind, beispielsweise Manpages, Dokumentationen und gemeinsam genutzte Binärversionen. Ein Failover kann jederzeit stattfinden, nachdem ein Dateisystem eingehängt wurde. Durch manuelles Einhängen können jetzt mehrere Replikationen aufgelistet werden,

ähnlich wie beim Automounter in Vorgängerversionen. Der Automounter bleibt bis auf eine Änderung unverändert: Es muss mit dem Failover nicht gewartet werden, bis das Dateisystem erneut eingehängt ist. Weitere Informationen finden Sie unter „So verwenden Sie das clientseitige Failover“ auf Seite 94 und „Clientseitiges Failover“ auf Seite 202.

Kerberos-Unterstützung für den NFS-Service

Solaris 2.0 unterstützt Kerberos-V4-Clients. In Version 2.6 wurden die Befehle `mount` und `share` geändert, um Einhängungen der NFS-Version 3 zu unterstützen, die die Kerberos-V5-Authentifizierung verwenden. Außerdem wurde der Befehl `share` geändert, um mehrere Authentifizierungsvarianten für verschiedene Clients bereitzustellen. Weitere Informationen zu Änderungen im Zusammenhang mit Sicherheitsvarianten finden Sie unter „RPCSEC_GSS-Sicherheitsvarianten“ auf Seite 82. Informationen zur Kerberos-V5-Authentifizierung finden Sie unter „Konfigurieren von Kerberos-NFS-Servern“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

WebNFS-Unterstützung

In Solaris 2.6 konnte auf ein Dateisystem im Internet über Firewalls zugegriffen werden. Dies war durch eine Erweiterung des NFS-Protokolls möglich. Einer der Vorteile des WebNFS-Protokolls für den Zugriff auf das Internet ist seine Zuverlässigkeit. Der Service ist eine Erweiterung des Protokolls der NFS-Versionen 3 und 2. Außerdem bietet die WebNFS-Implementierung die Möglichkeit der gemeinsamen Nutzung von Dateien ohne zusätzlichen Aufwand für die Verwaltung einer anonymen `FTP`-Site. Eine Beschreibung weiterer Änderungen im Zusammenhang mit dem WebNFS-Service finden Sie unter „Sicherheitsaushandlung für den WebNFS-Service“ auf Seite 83. Weitere aufgabenbezogene Informationen finden Sie unter „WebNFS-Systemverwaltungsaufgaben“ auf Seite 104.

Hinweis – Das Protokoll der NFS-Version 4 ist dem WebNFS-Service vorzuziehen. In der NFS-Version 4 sind sämtliche Sicherheitsfunktionen integriert, die in das MOUNT-Protokoll und den WebNFS-Service aufgenommen wurden.

RPCSEC_GSS-Sicherheitsvarianten

Die Sicherheitsvariante RPCSEC_GSS wird in Solaris 7 unterstützt. Bei dieser Variante werden die standardmäßigen GSS-API-Schnittstellen verwendet, um Authentifizierung, Integrität, Datenschutz sowie Unterstützung von mehreren Sicherheitsmechanismen zu gewährleisten. Weitere Informationen zur Unterstützung der Kerberos-V5-Authentifizierung finden Sie unter „Kerberos-Unterstützung für den NFS-Service“ auf Seite 82. Weitere Informationen zu GSS-API finden Sie unter *Developer's Guide to Oracle Solaris Security* .

Solaris 7-Erweiterungen für die NFS-Einhängung

Solaris 7 enthält Erweiterungen für die Befehle `mount` und `automountd`. Durch die Erweiterungen kann bei Einhängungsanforderungen die Routine für den Zugriff auf öffentliche Dateien anstelle des MOUNT-Protokolls verwendet werden. Das MOUNT-Protokoll verwendet dasselbe Zugriffsverfahren wie der WebNFS-Service. Durch Umgehen des MOUNT-Protokolls können Einhängungen über eine Firewall durchgeführt werden. Da weniger Transaktionen zwischen Server und Client stattfinden, wird das Einhängen beschleunigt.

Durch die Erweiterungen können zudem NFS-URLs anstelle von standardmäßigen Pfadnamen verwendet werden. Darüber hinaus können Sie die Option `public` in Verbindung mit dem Befehl `mount` und die Automounter-Maps verwenden, um die Verwendung der Routine für den Zugriff auf öffentliche Dateien zu erzwingen. Weitere Informationen über Änderungen am WebNFS-Service finden Sie unter „WebNFS-Unterstützung“ auf Seite 82.

Sicherheitsaushandlung für den WebNFS-Service

Ein neues Protokoll in Solaris 8 ermöglicht einem WebNFS-Client, einen Sicherheitsmechanismus mit einem NFS-Server auszuhandeln. Dieses Protokoll ermöglicht die Durchführung sicherer Transaktionen, wenn der WebNFS-Service verwendet wird. Weitere Informationen finden Sie unter „Funktionsweise der WebNFS-Sicherheitsaushandlung“ auf Seite 207.

NFS-Serverprotokollierung

In Solaris 8 ermöglicht die NFS-Serverprotokollierung einem NFS-Server, einen Protokoll der Vorgänge bereitzustellen, die in den Dateisystemen durchgeführt wurden. Dieser Protokoll enthält Informationen darüber, auf welche Datei zugegriffen wurde, wann auf die Datei zugegriffen wurde und welcher Benutzer auf die Datei zugegriffen hat. Anhand von verschiedenen Konfigurationsoptionen können Sie den Speicherort der Protokolle angeben, in denen diese Informationen enthalten sind. Außerdem können Sie diese Optionen verwenden, um die Vorgänge auszuwählen, die protokolliert werden sollen. Diese Funktion empfiehlt sich vor allem für Sites, auf denen anonyme FTP-Archive für NFS- und WebNFS-Clients zur Verfügung stehen. Weitere Informationen finden Sie unter „So aktivieren Sie die NFS-Serverprotokollierung“ auf Seite 89.

Hinweis – NFS-Version 4 bietet keine Unterstützung für die Serverprotokollierung.

Autofs-Funktionen

Autofs arbeitet mit Dateisystemen zusammen, die im lokalen Namespace angegeben sind. Diese Informationen können in NIS-, NIS+- oder lokalen Dateien enthalten sein.

In Solaris 2.6 ist eine umfassende Multithread-Version von `automountd` implementiert. Mit dieser Erweiterung wird autofs zuverlässiger. Außerdem ist die gleichzeitige Durchführung von mehreren Einhängungen möglich, wodurch verhindert wird, dass der Service ausfällt, wenn ein Server nicht verfügbar ist.

Das neue `automountd` verbessert zudem das bedarfsorientierte Einhängen. Bei früheren Versionen wurde eine komplette Gruppe von Dateisystemen eingehängt, wenn die Dateisysteme hierarchisch verbunden waren. Jetzt wird nur das Dateisystem der obersten Ebene eingehängt. Andere Dateisysteme, die am Einhängepunkt zur Verfügung stehen, können nach Bedarf eingehängt werden.

Der autofs-Service unterstützt die Durchsuchfunktion von indirekten Maps. Dadurch kann ein Benutzer feststellen, welche Verzeichnisse eingehängt werden können, ohne die jeweiligen Dateisysteme einzuhängen. Die autofs-Maps enthalten jetzt die Option `-nobrowse`, die bewirkt, dass große Dateisysteme wie beispielsweise `/net` und `/home` nicht automatisch durchsucht werden können. Zudem können Sie die autofs-Durchsuchfunktion für jeden Client deaktivieren, indem Sie die Option `-n` in Verbindung mit `automount` verwenden. Weitere Informationen finden Sie unter „Deaktivieren der autofs-Durchsuchfunktion“ auf Seite 122.

◆ ◆ ◆ KAPITEL 5

Verwaltung des Netzwerkdateisystems (Aufgaben)

Dieses Kapitel enthält Informationen zu NFS-Verwaltungsaufgaben wie beispielsweise das Einrichten von NFS-Services, das Hinzufügen neuer Dateisysteme zur gemeinsamen Nutzung und das Einhängen von Dateisystemen. Außerdem wird die Verwendung des Secure NFS-Systems und die Verwendung der WebNFS-Funktion behandelt. Im letzten Teil des Kapitels werden Fehlerbehebungsverfahren sowie NFS-Fehlermeldungen und deren Bedeutungen aufgeführt.

- „Automatische Freigabe von Dateisystemen“ auf Seite 86
- „Einhängen von Dateisystemen“ auf Seite 90
- „Einrichten von NFS-Services“ auf Seite 96
- „Verwalten des Secure NFS-Systems“ auf Seite 102
- „WebNFS-Systemverwaltungsaufgaben“ auf Seite 104
- „Aufgabenübersicht für die Autofs-Verwaltung“ auf Seite 107
- „Strategien für die NFS-Fehlerbehebung“ auf Seite 124
- „NFS-Fehlerbehebungsverfahren“ auf Seite 125
- „NFS-Fehlermeldungen“ auf Seite 135

Für welche Aufgaben Sie als NFS-Administrator verantwortlich sind, hängt von den Anforderungen Ihres Standorts und der Rolle Ihres Rechners im Netzwerk ab. Wenn Sie für alle Rechner im lokalen Netzwerk verantwortlich sind, treffen Sie möglicherweise auch folgende Entscheidungen:

- Welche Rechner als dedizierte Server eingesetzt werden
- Welche Rechner sowohl als Server wie auch als Client fungieren sollen
- Welche Rechner ausschließlich als Clients eingesetzt werden

Mit der Verwaltung eines Servers nach dessen Einrichtung sind folgende Aufgaben verbunden:

- Freigeben und Sperren von Dateisystemen
- Modifizieren von Administrationsdateien zum Aktualisieren der Dateisysteme, die von Ihrem Rechner freigegeben oder automatisch eingehängt werden
- Prüfen des Netzwerkstatus

- Diagnostizieren und Beheben von NFS-bezogenen Probleme, sobald diese auftreten
- Einrichten von Maps für autofs

Ein Rechner kann sowohl ein Server als auch ein Client sein. Aus diesem Grund kann ein Rechner verwendet werden, um lokale Dateisysteme für Remote-Rechner freizugeben und Remote-Dateisysteme einzuhängen.

Hinweis – Wenn auf Ihrem System aktivierte Zonen vorhanden sind und Sie beabsichtigen, diese Funktion in einer nicht globalen Zone zu verwenden, lesen Sie *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*, um weitere Informationen zu erhalten.

Automatische Freigabe von Dateisystemen

Auf die Dateisysteme von Servern kann zugegriffen werden, indem die Dateisysteme über die NFS-Umgebung freigegeben werden. Mithilfe des Befehls `share` oder der `/etc/dfs/dfstab`-Datei können Sie angeben, welche Dateisysteme für den gemeinsamen Dateizugriff freigegeben werden sollen.

Die Einträge in der `/etc/dfs/dfstab`-Datei werden automatisch gemeinsam genutzt, wenn Sie den NFS-Server starten. Sie sollten die automatische Freigabe einrichten, wenn dieselben Dateisysteme regelmäßig von verschiedenen Benutzern oder Systemen verwendet werden sollen. Wenn Ihr Rechner beispielsweise ein Server ist, der Home-Verzeichnisse unterstützt, müssen die Home-Verzeichnisse jederzeit zur Verfügung stehen. Meist sollten Dateisysteme automatisch freigegeben werden. Eine manuelle Freigabe sollte nur während der Durchführung von Prüfungen oder Fehlerbehebungsverfahren stattfinden.

Die Datei `dfstab` dient zum Auflisten aller Dateisysteme, die von Ihrem Server und dessen Clients gemeinsam genutzt werden. Diese Datei steuert zudem, welche Clients ein Dateisystem einhängen können. Sie können `dfstab` modifizieren, um ein Dateisystem hinzuzufügen oder zu löschen oder um die Art und Weise der Freigabe zu ändern. Dazu müssen Sie nur die Datei mit einem unterstützten Texteditor (wie beispielsweise `vi`) bearbeiten. Wenn der Rechner beim nächsten Mal auf die Betriebsebene 3 wechselt, wird die aktualisierte Datei `dfstab` gelesen, wodurch festgestellt wird, welches Dateisystem automatisch gemeinsam genutzt werden kann.

Jede Zeile der Datei `dfstab` enthält einen Freigabebefehl (`share`). Einen solchen Befehl geben Sie auf der Befehlszeile ein, um das Dateisystem gemeinsam zu nutzen. Der `share`-Befehl befindet sich in `/usr/sbin`.

TABELLE 5–1 Übersicht der Schritte für gemeinsame Nutzung von Dateisystemen

Aufgabe	Beschreibung	Siehe
Einrichten der automatischen Freigabe von Dateisystemen	Schritte zum Konfigurieren eines Servers, damit Dateisysteme automatisch gemeinsam genutzt werden, wenn der Server neu gestartet wird	„So richten Sie die automatische Freigabe von Dateisystemen ein“ auf Seite 87
Aktivieren von WebNFS	Schritte zum Konfigurieren eines Servers, damit Benutzer mithilfe von WebNFS auf Dateien zugreifen können	„So aktivieren Sie den WebNFS-Zugang“ auf Seite 88
Aktivieren der NFS-Serverprotokollierung	Schritte zum Konfigurieren eines Servers, damit die NFS-Protokollierung auf ausgewählten Dateisystemen ausgeführt wird	„So aktivieren Sie die NFS-Serverprotokollierung“ auf Seite 89

▼ So richten Sie die automatische Freigabe von Dateisystemen ein

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie Einträge für jedes Dateisystem hinzu, das gemeinsam genutzt werden soll.**

Bearbeiten Sie `/etc/dfs/dfstab` . Fügen Sie für jedes Dateisystem, das automatisch gemeinsam genutzt werden soll, einen Eintrag in die Datei ein. Jeder Eintrag muss sich auf einer separaten Zeile befinden und folgende Syntax haben:

```
share [-F nfs] [-o specific-options] [-d description] pathname
```

Auf der Manpage `dfstab(4)` finden Sie eine Beschreibung von `/etc/dfs/dfstab`, und auf der Manpage `share_nfs(1M)` finden Sie eine vollständige Liste der Optionen.

3 **Geben Sie das Dateisystem für die gemeinsame Nutzung frei.**

Sobald der Eintrag in `/etc/dfs/dfstab` eingefügt ist, können Sie das Dateisystem gemeinsam nutzen, indem Sie entweder das System neu starten oder den Befehl `shareall` ausführen.

```
# shareall
```

4 **Prüfen Sie, ob die Informationen korrekt sind.**

Führen Sie den Befehl `share` aus, um sicherzustellen, dass die richtigen Optionen aufgelistet sind:

```
# share
-        /export/share/man   ro   ""
-        /usr/src     rw=eng   ""
-        /export/ftp    ro,public  ""
```

Siehe auch Als Nächstes richten Sie Ihre autofs-Maps ein, damit die Clients auf die Dateisysteme zugreifen können, die Sie auf dem Server für die gemeinsame Nutzung freigegeben haben. Lesen Sie dazu „Aufgabenübersicht für die Autofs-Verwaltung“ auf Seite 107.

▼ So aktivieren Sie den WebNFS-Zugang

Ab Solaris 2.6 stehen alle Dateisysteme, die für die NFS-Einhängung zur Verfügung stehen, automatisch für den WebNFS-Zugang bereit. Die einzigen Bedingungen, die eine Durchführung dieses Verfahrens erfordern, sind folgende:

- Zulassen des Einhängens mit NFS auf einem Server, bei dem dies noch nicht möglich ist
- Rücksetzen der Routine für den Zugriff auf öffentliche Dateien, um NFS-URLs mithilfe der Option `public` zu kürzen
- Erzwingen des Ladens einer spezifischen HTML-Datei mithilfe der Option `index`

Faktoren, die vor dem Starten des WebNFS-Service zu berücksichtigen sind, finden Sie unter „Planung für den WebNFS-Zugriff“ auf Seite 105.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie Einträge für jedes Dateisystem hinzu, das mithilfe des WebNFS-Service gemeinsam genutzt werden soll.

Bearbeiten Sie `/etc/dfs/dfstab`. Fügen Sie für jedes Dateisystem einen Eintrag in die Datei ein. Die im folgenden Beispiel gezeigten Tags `public` und `index` sind optional.

```
share -F nfs -o ro,public,index=index.html /export/ftp
```

Auf der Manpage `dfstab(4)` finden Sie eine Beschreibung von `/etc/dfs/dfstab`, und auf der Manpage `share_nfs(1M)` finden Sie eine vollständige Liste der Optionen.

3 Geben Sie das Dateisystem für die gemeinsame Nutzung frei.

Sobald der Eintrag in `/etc/dfs/dfstab` eingefügt ist, können Sie das Dateisystem gemeinsam Nutzen, indem Sie entweder das System neu starten oder den Befehl `shareall` ausführen.

```
# shareall
```

4 Prüfen Sie, ob die Informationen korrekt sind.

Führen Sie den Befehl `share` aus, um sicherzustellen, dass die richtigen Optionen aufgelistet sind:

```
# share
-       /export/share/man   ro   ""
-       /usr/src     rw=eng   ""
-       /export/ftp    ro,public,index=index.html  ""
```

So aktivieren Sie die NFS-Serverprotokollierung

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **(Optional) Ändern Sie die Konfigurationseinstellungen des Dateisystems.**

   Sie haben zwei Möglichkeiten, die Einstellungen in `/etc/nfs/nfslog.conf` zu ändern. Sie können die Standardeinstellungen für alle Dateisysteme bearbeiten, indem Sie die Daten ändern, die dem `global` -Tag zugeordnet sind. Sie können aber auch ein neues Tag für dieses Dateisystem hinzufügen. Wenn diese Änderungen nicht nötig sind, müssen Sie diese Datei nicht ändern. Das Format von `/etc/nfs/nfslog.conf` wird in `nfslog.conf(4)` beschrieben.

3. **Fügen Sie Einträge für jedes Dateisystem hinzu, das mithilfe der NFS-Serverprotokollierung zur gemeinsamen Nutzung freigegeben werden soll.**

   Bearbeiten Sie `/etc/dfs/dfstab`. Fügen Sie für jedes Dateisystem, für das Sie die NFS-Serverprotokollierung aktivieren, einen Eintrag in die Datei ein. Das Tag, das zusammen mit der Option `log=`*tag* verwendet wird, muss in `/etc/nfs/nfslog.conf` eingetragen werden. Im folgenden Beispiel werden die Standardeinstellungen im `global`-Tag verwendet.

   ```
   share -F nfs -o ro,log=global /export/ftp
   ```

   Auf der Manpage `dfstab(4)` finden Sie eine Beschreibung von `/etc/dfs/dfstab`, und auf der Manpage `share_nfs(1M)` finden Sie eine vollständige Liste der Optionen.

4. **Geben Sie das Dateisystem für die gemeinsame Nutzung frei.**

   Sobald der Eintrag in `/etc/dfs/dfstab` eingefügt ist, können Sie das Dateisystem gemeinsam nutzen, indem Sie entweder das System neu starten oder den Befehl `shareall` ausführen.

   ```
   # shareall
   ```

5. **Prüfen Sie, ob die Informationen korrekt sind.**

   Führen Sie den Befehl `share` aus, um sicherzustellen, dass die richtigen Optionen aufgelistet sind:

   ```
   # share
   -        /export/share/man   ro   ""
   -        /usr/src     rw=eng   ""
   -        /export/ftp    ro,log=global  ""
   ```

6. **Prüfen Sie, ob `nfslogd`, der NFS-Protokolldämon, ausgeführt wird.**

   ```
   # ps -ef | grep nfslogd
   ```

7 **(Optional) Starten Sie den Dämon `nfslogd`, falls er noch nicht gestartet wurde.**

- **(Optional) Wenn `/etc/nfs/nfslogtab` vorhanden ist, starten Sie den NFS-Protokolldämon, indem Sie Folgendes eingeben:**

  ```
  # svcadm restart network/nfs/server:default
  ```

- **(Optional) Wenn `/etc/nfs/nfslogtab` nicht vorhanden ist, führen Sie einen der `share`-Befehle aus, um die Datei zu erstellen, und starten Sie dann den Dämon.**

  ```
  # shareall
  # svcadm restart network/nfs/server:default
  ```

Einhängen von Dateisystemen

Sie haben verschiedene Möglichkeiten, um Dateisysteme einzuhängen. Dateisysteme können automatisch eingehängt werden, wenn das System neu gestartet wird, nach Bedarf über die Befehlszeile, oder mithilfe des Automounters. Der Automounter bietet viele Vorteile für das Einhängen während des Boot-Vorgangs oder über die Befehlszeile. In manchen Situationen ist jedoch eine Kombination aller drei Verfahren nötig. Außerdem gibt es mehrere Möglichkeiten der Aktivierung oder Deaktivierung, was von den Optionen abhängt, die Sie zum Einhängen des Dateisystems verwenden. In der folgenden Tabelle sind sämtliche Aufgaben aufgeführt, die mit dem Einhängen von Dateisystemen zusammenhängen.

TABELLE 5–2 Übersicht der Schritte für das Einhängen von Dateisystemen

Aufgabe	Beschreibung	Siehe
Einhängen eines Dateisystems während des Boot-Vorgangs	Schritte zum Einhängen eines Dateisystem während des Boot-Vorgangs eines Systems	„So hängen Sie ein Dateisystem während des Boot-Vorgangs ein“ auf Seite 91.
Einhängen eines Dateisystems mithilfe eines Befehls	Schritte zum Einhängen eines Dateisystems, während ein System ausgeführt wird. Dieses Verfahren ist für Prüfzwecke nützlich.	„So hängen Sie ein Dateisystem über die Befehlszeile ein“ auf Seite 92.
Einhängen mit dem Automounter	Schritte zum Zugreifen auf ein Dateisystem ohne Verwendung der Befehlszeile	„Einhängen mit dem Automounter“ auf Seite 92.
Verhindern der Erstellung großer Dateien	Schritte zum Verhindern, dass in einem Dateisystem große Dateien erstellt werden	„So deaktivieren Sie große Dateien auf einem NFS-Server“ auf Seite 93.
Starten des clientseitigen Failover	Schritte zum automatischen Umschalten auf ein funktionierendes Dateisystem, wenn ein Server ausfällt	„So verwenden Sie das clientseitige Failover“ auf Seite 94.
Deaktivieren des Einhängezugriffs eines Clients	Schritte zum Deaktivieren der Fähigkeit eines Clients, auf ein Remote-Dateisystem zuzugreifen	„So deaktivieren Sie den Einhängezugriff eines Clients“ auf Seite 94.

TABELLE 5–2 Übersicht der Schritte für das Einhängen von Dateisystemen *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Ermöglichen des Zugriffs auf ein Dateisystem über eine Firewall	Schritte zur Zulassung des Zugriffs auf ein Dateisystem über eine Firewall mithilfe des WebNFS-Protokolls	„So hängen Sie ein NFS-Dateisystem über eine Firewall ein“ auf Seite 95.
Einhängen eines Dateisystems mithilfe einer NFS-URL	Schritte zur Zulassung des Zugriffs auf ein Dateisystem mithilfe einer NFS-URL. Dieses Verfahren ermöglicht den Zugriff auf das Dateisystem ohne Verwendung des MOUNT-Protokolls.	„So hängen Sie ein NFS-Dateisystem mithilfe einer NFS-URL ein“ auf Seite 95.

▼ So hängen Sie ein Dateisystem während des Boot-Vorgangs ein

Richten Sie sich nach dem nachstehenden Verfahren, um während des Boot-Vorgangs Dateisysteme einzuhängen anstatt autofs-Maps zu verwenden. Dieses Verfahren muss für jeden Client ausgeführt werden, der Zugriff auf Remote-Dateisysteme haben soll.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie einen Eintrag für das Dateisystem in `/etc/vfstab` ein.**

Einträge in der `/etc/vfstab` -Datei haben die folgende Syntax:

```
special  fsckdev  mountp  fstype  fsckpass  mount-at-boot  mntopts
```

Weitere Informationen finden Sie auf der Manpage `vfstab(4)`.

Achtung – Bei NFS-Servern, die auch `vfstab`-Einträge von NFS-Clients aufweisen, muss stets die Option `bg` angegeben sein, um zu vermeiden, dass das System beim Boot-Vorgang hängenbleibt. Weitere Informationen finden Sie unter „`mount`-Optionen für NFS-Dateisysteme“ auf Seite 163.

Beispiel 5–1 Eintrag in der `vfstab`-Datei des Clients

Sie beabsichtigen, einen Clientrechner zu verwenden, um das `/var/mail`-Verzeichnis des Servers `wasp` einzuhängen. Das Dateisystem soll als `/var/mail` auf dem Client eingehängt werden, und der Client soll Lese- und Schreibzugriff haben. Fügen Sie den folgenden Eintrag in die `vfstab`-Datei des Clients ein:

```
wasp:/var/mail - /var/mail nfs - yes rw
```

▼ So hängen Sie ein Dateisystem über die Befehlszeile ein

Das Einhängen eines Dateisystems über die Befehlszeile wird oft durchgeführt, um einen neuen Einhängepunkt zu testen. Diese Art des Einhängens erlaubt den vorübergehenden Zugriff auf ein Dateisystem, auf das nicht über den Automounter zugegriffen werden kann.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Hängen Sie das Dateisystem ein.

Geben Sie den folgenden Befehl ein:

```
# mount -F nfs -o ro bee:/export/share/local /mnt
```

In diesem Fall wird das `/export/share/local`-Dateisystem vom Server `bee` im schreibgeschützten `/mnt` auf dem lokalen System eingehängt. Das Einhängen über die Befehlszeile ermöglicht es, ein Dateisystem vorübergehend anzuzeigen. Sie können das Dateisystem mit `umount` aushängen oder den lokalen Host neu starten.

Achtung – Bei keiner Version des Befehls `mount` wird nicht vor ungültigen Optionen gewarnt. Bei Verwendung des Befehls werden stillschweigend alle Optionen ignoriert, die nicht interpretiert werden können. Überprüfen Sie alle verwendeten Optionen, um ein unerwartetes Verhalten zu vermeiden.

Einhängen mit dem Automounter

Unter „Aufgabenübersicht für die Autofs-Verwaltung“ auf Seite 107 finden Sie spezielle Anweisungen für die Einrichtung und die Unterstützung des Einhängens mit dem Automounter. Clients sollten über den `/net`-Einhängepunkt auf Remote-Dateisysteme zugreifen können, ohne dass Änderungen am generischen System nötig sind. Um das im vorangegangenen Beispiel aufgeführte `/export/share/local`-Dateisystem einzuhängen, geben Sie Folgendes ein:

```
% cd /net/bee/export/share/local
```

Da der Automounter allen Benutzern erlaubt, Dateisysteme einzuhängen, ist kein `root`-Zugriff erforderlich. Da der Automounter auch für das automatische Aushängen von Dateisystemen sorgt, müssen Sie keine Dateisysteme aushängen, wenn Sie den Vorgang abgeschlossen haben.

▼ So deaktivieren Sie große Dateien auf einem NFS-Server

Bei Servern, die Clients unterstützen, die keine Dateien mit einer Größe von mehr als 2 GB verarbeiten können, können Sie die Funktion zum Erstellen von großen Dateien deaktivieren.

Hinweis – Bei Versionen, die älter als Solaris 2.6 sind, können keine großen Dateien verwendet werden. Wenn die Clients auf große Dateien zugreifen müssen, muss auf den Clients des NFS-Servers mindestens die Version 2.6 von Solaris ausgeführt werden.

---

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stellen Sie sicher, dass im Dateisystem keine großen Dateien vorhanden sind.

Beispiel:

```
# cd /export/home1
# find . -xdev -size +2000000 -exec ls -l {} \;
```

Wenn große Dateien im Dateisystem vorhanden sind, müssen Sie diese Dateien entfernen oder in ein anderes Dateisystem verschieben.

3 Hängen Sie das Dateisystem aus.

```
# umount /export/home1
```

4 Setzen Sie das Dateisystem auf seinen ursprünglichen Zustand zurück, wenn es mithilfe von `largefiles` eingehängt wurde.

Mit `fsck` wird das Dateisystem zurückgesetzt, wenn keine großen Dateien im Dateisystem vorhanden sind:

```
# fsck /export/home1
```

5 Hängen Sie das Dateisystem mithilfe von `nolargefiles` ein.

```
# mount -F ufs -o nolargefiles /export/home1
```

Sie können das Dateisystem über die Befehlszeile einhängen. Um diese Option jedoch als dauerhafte Option festzulegen, fügen Sie einen Eintrag wie den folgenden in `/etc/vfstab` ein:

```
/dev/dsk/c0t3d0s1 /dev/rdsk/c0t3d0s1 /export/home1  ufs  2  yes  nolargefiles
```

▼ So verwenden Sie das clientseitige Failover

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Hängen Sie das Dateisystem auf dem NFS-Client ein, indem Sie die Option `ro` verwenden.**

Sie können das Dateisystem über die Befehlszeile, über den Automounter oder durch Einfügen eines Eintrags in `/etc/vfstab` einhängen, der folgende Syntax hat:

```
bee,wasp:/export/share/local  -  /usr/local  nfs  -  no  ro
```

Diese Syntax wurde vom Automounter zugelassen. Das Failover war jedoch nicht während des Einhängens von Dateisystemen verfügbar, sondern nur dann, wenn ein Server ausgewählt wurde.

Hinweis – Server, auf denen verschiedene Versionen von NFS-Protokollen ausgeführt werden, können nicht über die Befehlszeile oder mithilfe eines `vfstab`-Eintrags kombiniert werden. Server, die Protokolle der NFS-Version 2, 3 oder 4 unterstützen, können nur mithilfe von autofs kombiniert werden. In autofs werden die geeignetsten Server der Version 2, 3 oder 4 verwendet.

▼ So deaktivieren Sie den Einhängezugriff eines Clients

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie einen Eintrag in `/etc/dfs/dfstab` ein.**

Im ersten Beispiel wird allen Clients in der Netzgruppe `eng` der Zugriff für das Einhängen gestattet, mit Ausnahme des Hosts namens `rose`. Im zweiten Beispiel wird allen Clients in der DNS-Domain `eng.example.com` der Zugriff für das Einhängen gestattet, mit Ausnahme von `rose`.

```
share -F nfs -o ro=-rose:eng /export/share/man
share -F nfs -o ro=-rose:.eng.example.com /export/share/man
```

Weitere Informationen zu den Zugriffslisten finden Sie unter „Einrichten von Zugriffslisten mit dem `share`-Befehl“ auf Seite 175. Eine Beschreibung von `/etc/dfs/dfstab` finden Sie unter `dfstab`(4).

3 **Geben Sie das Dateisystem für die gemeinsame Nutzung frei.**

Der NFS-Server verwendet die Änderungen in `/etc/dfs/dfstab` erst dann, wenn die Dateisysteme wieder gemeinsam genutzt werden können oder der Server neu gestartet wird.

```
# shareall
```

▼ So hängen Sie ein NFS-Dateisystem über eine Firewall ein

Um über eine Firewall auf Dateisysteme zuzugreifen, gehen Sie wie folgt vor:

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Hängen Sie das Dateisystem manuell ein, indem Sie einen Befehl wie den folgenden verwenden:**

```
# mount -F nfs bee:/export/share/local /mnt
```

In diesem Beispiel wird das Dateisystem `/export/share/local` auf dem lokalen Client eingehängt, indem die Routine für den Zugriff auf öffentliche Dateien verwendet wird. Anstelle des standardmäßigen Pfadnamens kann eine NFS-URL verwendet werden. Wenn die Routine für den Zugriff auf öffentliche Dateien nicht vom Server `bee` unterstützt wird, schlägt das Einhängen fehl.

Hinweis – Damit dieses Verfahren durchgeführt werden kann, muss das Dateisystem auf dem NFS-Server mithilfe der Option `public` für die gemeinsame Nutzung freigegeben werden. Außerdem müssen Firewalls, die sich zwischen Client und Server befinden, TCP-Verbindungen am Port `2049` zulassen. Alle gemeinsam genutzte Dateisysteme lassen den Zugriff auf öffentliche Dateien zu. Aus diesem Grund ist die Option `public` standardmäßig aktiviert.

▼ So hängen Sie ein NFS-Dateisystem mithilfe einer NFS-URL ein

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **(Optional) Wenn Sie NFS-Version 2 oder 3 verwenden, hängen Sie das Dateisystem manuell ein, indem Sie einen Befehl wie den folgenden verwenden:**

```
# mount -F nfs nfs://bee:3000/export/share/local /mnt
```

In diesem Beispiel wird das `/export/share/local` -Dateisystem vom Server `bee` mithilfe der NFS-Portnummer `3000` eingehängt. Die Portnummer wird nicht benötigt, und die standardmäßige NFS-Portnummer `2049` wird verwendet. Für eine NFS-URL können Sie die Option `public` verwenden. Ohne die Option `public` wird das MOUNT-Protokoll verwendet, wenn die Routine für den Zugriff auf öffentliche Dateien nicht vom Server unterstützt wird. Durch die Option `public` wird die Verwendung der Routine für den Zugriff auf öffentliche Dateien erzwungen. Das Einhängen schlägt fehl, wenn die Routine für den Zugriff auf öffentliche Dateien nicht unterstützt wird.

3 **(Optional) Wenn Sie NFS-Version 4 verwenden, hängen Sie das Dateisystem manuell ein, indem Sie einen Befehl wie den folgenden verwenden:**

```
# mount -F nfs -o vers=4 nfs://bee:3000/export/share/local /mnt
```

Einrichten von NFS-Services

In diesem Abschnitt werden einige der Aufgaben beschrieben, die für Folgendes benötigt werden:

- Starten und Stoppen des NFS-Servers
- Starten und Stoppen des Automounters
- Auswählen einer anderen NFS-Version

Hinweis – Ab Solaris 10 ist die NFS-Version 4 die Standardversion.

TABELLE 5–3 Übersicht der Schritte für NFS-Services

Aufgabe	Beschreibung	Siehe
Starten des NFS-Servers	Schritte zum Starten des NFS-Service, sofern er nicht automatisch gestartet wurde	„So starten Sie die NFS-Services“ auf Seite 97
Stoppen des NFS-Servers	Schritte zum Stoppen des NFS-Service. Normalerweise ist es nicht nötig, den Service zu stoppen.	„So stoppen Sie die NFS-Services“ auf Seite 98
Starten des Automounters	Schritte zum Starten des Automounters. Dieses Verfahren ist erforderlich, wenn Maps des Automounters geändert werden.	„So starten Sie den Automounter“ auf Seite 98
Stoppen des Automounters	Schritte zum Stoppen des Automounters. Dieses Verfahren ist erforderlich, wenn Maps des Automounters geändert werden.	„So stoppen Sie den Automounter“ auf Seite 98

TABELLE 5–3 Übersicht der Schritte für NFS-Services *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Auswählen einer anderen NFS-Version auf dem Server	Schritte zum Auswählen einer anderen NFS-Version auf dem Server. Richten Sie sich nach diesem Verfahren, wenn die NFS-Version 4 nicht verwendet werden soll.	„So wählen Sie andere NFS-Versionen auf einem Server aus“ auf Seite 99
Auswählen einer anderen NFS-Version auf dem Client	Schritte zum Auswählen einer anderen NFS-Version auf dem Client durch Modifizieren der `/etc/default/nfs`-Datei. Richten Sie sich nach diesem Verfahren, wenn die NFS-Version 4 nicht verwendet werden soll.	„So wählen Sie andere NFS-Versionen auf einem Client aus, indem Sie die `/etc/default/nfs`-Datei modifizieren“ auf Seite 100
	Alternative Schritte zum Auswählen einer anderen NFS-Version auf dem Client durch Verwenden der Befehlszeile. Wenden Sie dieses alternative Verfahren an, wenn die NFS-Version 4 nicht verwendet werden soll.	„Verwenden des `mount`-Befehls zum Auswählen anderer Versionen von NFS auf einem Client“ auf Seite 101

▼ So starten Sie die NFS-Services

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Aktivieren Sie den NFS-Service auf dem Server.**

   Geben Sie folgenden Befehl ein:

   ```
   # svcadm enable network/nfs/server
   ```

   Durch diesen Befehl wird der NFS-Service aktiviert.

Hinweis – Der NFS-Server wird automatisch gestartet, wenn Sie das System starten. Außerdem können die NFS-Servicedämonen nach jedem Neustart des Systems automatisch aktiviert werden, indem das NFS-Dateisystem freigegeben wird. Informationen zur Vorgehensweise finden Sie unter „So richten Sie die automatische Freigabe von Dateisystemen ein“ auf Seite 87.

▼ So stoppen Sie die NFS-Services

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Deaktivieren Sie den NFS-Service auf dem Server.**

Geben Sie folgenden Befehl ein:

```
# svcadm disable network/nfs/server
```

▼ So starten Sie den Automounter

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Aktivieren Sie den autofs-Dämon.**

Geben Sie folgenden Befehl ein:

```
# svcadm enable system/filesystem/autofs
```

▼ So stoppen Sie den Automounter

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Deaktivieren Sie den autofs-Dämon.**

Geben Sie folgenden Befehl ein:

```
# svcadm disable system/filesystem/autofs
```

▼ So wählen Sie andere NFS-Versionen auf einem Server aus

Richten Sie sich nach diesem Verfahren, wenn die NFS-Version 4 nicht verwendet werden soll.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Bearbeiten Sie die `/etc/default/nfs`-Datei.**

Wenn der Server beispielsweise nur Version 3 bereitstellen soll, setzen Sie die Werte von NFS_SERVER_VERSMAX und NFS_SERVER_VERSMIN auf 3. Eine Liste der Schlüsselwörter und der zugehörigen Werte finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144.

```
NFS_SERVER_VERSMAX=value
NFS_SERVER_VERSMIN=value
```

value Stellt die Versionsnummer bereit.

Hinweis – Diese Zeilen werden standardmäßig kommentiert. Vergessen Sie nicht, das Nummernzeichen (#) zu entfernen.

---

3 **(Optional) Um die Serverdelegierung zu deaktivieren, fügen Sie die folgende Zeile in die `/etc/default/nfs`-Datei ein:**

```
NFS_SERVER_DELEGATION=off
```

Hinweis – In NFS-Version 4 ist die Serverdelegierung standardmäßig aktiviert. Weitere Informationen finden Sie unter „Delegierung in NFS-Version 4“ auf Seite 195.

---

4 **(Optional) Um eine allgemeine Domain für Clients und Server festzulegen, fügen Sie die folgende Zeile in die `/etc/default/nfs`-Datei ein:**

```
NFSMAPID_DOMAIN=my.comany.com
```

my.comany.com Bereitstellung der allgemeinen Domain

Weitere Informationen finden Sie unter „`nfsmapid`-Dämon“ auf Seite 151.

5 **Prüfen Sie, ob der NFS-Service auf dem Server ausgeführt wird.**

Geben Sie folgenden Befehl ein:

```
# svcs network/nfs/server
```

Mithilfe dieses Befehls wird festgestellt, ob der NFS-Serverservice online oder deaktiviert ist.

6 **(Optional) Deaktivieren Sie bei Bedarf den NFS-Service.**

Wenn Sie während der Ausführung des vorangegangenen Schritts festgestellt haben, dass der NFS-Service online ist, geben Sie den folgenden Befehl ein, um den Service zu deaktivieren:

```
# svcadm disable network/nfs/server
```

Hinweis – Wenn Sie Ihren NFS-Service konfigurieren müssen, informieren Sie sich unter „So richten Sie die automatische Freigabe von Dateisystemen ein“ auf Seite 87.

---

7 **Aktivieren Sie den NFS-Service.**

Geben Sie folgenden Befehl ein, um den Service zu aktivieren:

```
# svcadm enable network/nfs/server
```

Siehe auch „Versionsaushandlung in NFS“ auf Seite 187

▼ So wählen Sie andere NFS-Versionen auf einem Client aus, indem Sie die `/etc/default/nfs`-Datei modifizieren

Das folgende Verfahrens dient zum Kontrollieren der NFS-Version, die auf dem Client verwendet wird, indem die `/etc/default/nfs`-Datei modifiziert wird. Informationen zum Verwenden der Befehlszeile finden Sie unter „Verwenden des `mount`-Befehls zum Auswählen anderer Versionen von NFS auf einem Client“ auf Seite 101.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Bearbeiten Sie die `/etc/default/nfs`-Datei.**

Wenn nur Version 3 auf dem Client bereitgestellt werden soll, setzen Sie die Werte für NFS_CLIENT_VERSMAX und NFS_CLIENT_VERSMIN auf 3. Eine Liste der Schlüsselwörter und der zugehörigen Werte finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144.

```
NFS_CLIENT_VERSMAX=value
NFS_CLIENT_VERSMIN=value
```

value Stellt die Versionsnummer bereit.

Hinweis – Diese Zeilen werden standardmäßig kommentiert. Vergessen Sie nicht, das Nummernzeichen (#) zu entfernen.

3 Hängen Sie NFS auf dem Client ein.

Geben Sie folgenden Befehl ein:

```
# mount server-name:/share-point /local-dir
```

server-name Stellt den Namen des Servers bereit.

/share-point Stellt den Pfad des Remote-Verzeichnisses bereit, das gemeinsam genutzt werden soll.

/local-dir Stellt den Pfad des lokalen Einhängepunkts bereit.

Siehe auch „Versionsaushandlung in NFS“ auf Seite 187

▼ Verwenden des `mount`-Befehls zum Auswählen anderer Versionen von NFS auf einem Client

Anhand des folgenden Verfahrens kann mithilfe des `mount`-Befehls bestimmt werden, welche NFS-Version auf einem Client für einen bestimmten Einhängevorgang verwendet wird. Informationen zum Ändern der NFS-Version für alle von Clients eingehängten Dateisysteme finden Sie unter „So wählen Sie andere NFS-Versionen auf einem Client aus, indem Sie die `/etc/default/nfs`-Datei modifizieren“ auf Seite 100.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Hängen Sie die gewünschte NFS-Version auf dem Client ein.

Geben Sie folgenden Befehl ein:

```
# mount -o vers=value server-name:/share-point /local-dir
```

value Stellt die Versionsnummer bereit.

server-name Stellt den Namen des Servers bereit.

/share-point Stellt den Pfad des Remote-Verzeichnisses bereit, das gemeinsam genutzt werden soll.

/local-dir Stellt den Pfad des lokalen Einhängepunkts bereit.

Hinweis – Wenn dieser Befehl ausgeführt wird, wird das NFS-Protokoll verwendet, um das Remote-Verzeichnis einzuhängen, und die Clienteinstellungen in der `/etc/default/nfs`-Datei werden außer Kraft gesetzt.

Siehe auch „Versionsaushandlung in NFS“ auf Seite 187

Verwalten des Secure NFS-Systems

Damit das Secure NFS-System verwendet werden kann, müssen alle von Ihnen verwalteten Rechner einen Domainnamen haben. Eine Domain ist eine Entität zur Systemverwaltung, die aus mehreren Rechnern besteht und zu einem größeren Netzwerk gehört. Wenn Sie einen Name Service ausführen, sollten Sie auch einen Name Service für die Domain einrichten. Lesen Sie dazu *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*.

Die Kerberos-V5-Authentifizierung wird vom NFS-Service unterstützt. Eine Erläuterung des Kerberos-Service finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Sie können auch die Secure NFS-Umgebung konfigurieren, um die Diffie-Hellman-Authentifizierung zu verwenden. Eine Erläuterung dieses Authentifizierungsservice finden Sie in Kapitel 16, „Verwenden von Authentifizierungsservices (Aufgaben)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

▼ So Richten Sie eine Secure NFS-Umgebung mit DH-Authentifizierung ein

1. **Weisen Sie Ihrer Domain einem Domainnamen zu, und sorgen Sie dafür, dass der Domainname jedem Rechner in der Domain bekannt ist.**

   Wenn Sie NIS+ als Name Service verwenden, informieren Sie sich im *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*.

2. **Erstellen Sie öffentliche und geheime Schlüssel für die Benutzer Ihrer Clients, indem Sie den Befehl `newkey` oder den Befehl `nisaddcred` verwenden. Lassen Sie von jedem Benutzer ein eigenes RPC-Passwort mithilfe des Befehls `chkey` erstellen.**

Hinweis – Informationen zu diesen Befehlen finden Sie auf den Manpages newkey(1M), nisaddcred(1M) und chkey(1).

Nachdem öffentliche und geheime Schlüssel erstellt wurden, werden die öffentlichen und verschlüsselten geheimen Schlüssel in der publickey-Datenbank gespeichert.

3 Stellen Sie sicher, dass der Name Service reagiert.

Wenn Sie NIS+ verwenden, geben Sie Folgendes ein:

```
# nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-replica-58.acme.com.
        Last Update seen was Mon Jun  5 11:16:10 1995
```

Wenn Sie NIS verwenden, stellen Sie sicher, dass der ypbind-Dämon ausgeführt wird.

4 Stellen Sie sicher, dass der keyserv-Dämon des Schlüsselservers ausgeführt wird.

Geben Sie folgenden Befehl ein:

```
# ps -ef | grep keyserv
root    100      1  16    Apr 11 ?        0:00 /usr/sbin/keyserv
root   2215   2211   5  09:57:28 pts/0    0:00 grep keyserv
```

Wenn der Dämon nicht ausgeführt wird, starten Sie den Schlüsselserver, indem Sie Folgendes eingeben:

```
# /usr/sbin/keyserv
```

5 Entschlüsseln und speichern Sie die Geheimnisdatei.

Normalerweise ist das Anmeldepasswort identisch mit dem Netzwerkpasswort. In diesem Fall ist keylogin nicht erforderlich. Wenn sich die Passwörter unterscheiden, müssen sich die Benutzer anmelden und dann keylogin ausführen. Sie müssen den Befehl keylogin -r als root-Benutzer ausführen , um den entschlüsselten Geheimnisschlüssel in /etc/.rootkey zu speichern.

Hinweis – Sie müssen keylogin -r ausführen, wenn der Root-Geheimnisschlüssel sich geändert hat oder wenn /etc/.rootkey verloren gegangen ist.

6 Aktualisieren Sie die Einhängeoptionen für das Dateisystem.

Für die Diffie-Hellman-Authentifizierung bearbeiten Sie die /etc/dfs/dfstab-Datei und fügen die Option sec=dh zu den entsprechenden Einträgen hinzu.

```
share -F nfs -o sec=dh /export/home
```

Auf der Manpage dfstab(4) finden Sie eine Beschreibung von /etc/dfs/dfstab.

7 Aktivieren Sie die Automounter-Maps für das Dateisystem.

Bearbeiten Sie `auto_master`-Daten, um `sec=dh` als Einhängeoption in die entsprechenden Einträge für die Diffie-Hellman-Authentifizierung einzufügen:

```
/home     auto_home     -nosuid,sec=dh
```

Hinweis – Die Versionen bis Solaris 2.5 weisen eine Beschränkung auf. Wenn ein Client ein sicheres gemeinsam genutztes Dateisystem nicht sicher einhängt, haben Benutzer als `nobody` anstelle ihres eigenen Benutzernames Zugriff. Bei nachfolgenden Versionen, die Version 2 verwenden, verweigert der NFS-Server den Zugriff, wenn die Sicherheitsmodi nicht übereinstimmen, es sei denn, `-sec=none` ist auf der `share`-Befehlszeile angegeben. Bei Version 3 wird der Modus vom NFS-Server übernommen, sodass `sec=dh` nicht von den Clients angegeben werden muss. Die Benutzer können mit ihrem eigenen Benutzernamen auf die Dateien zugreifen.

Um einen Rechner neu zu installieren, zu verschieben oder zu aktualisieren, müssen Sie `/etc/.rootkey` speichern, wenn Sie weder neue Schlüssel erstellen noch Schlüssel für `root` ändern. Wenn Sie `/etc/.rootkey` löschen, können Sie Folgendes eingeben:

```
# keylogin -r
```

WebNFS-Systemverwaltungsaufgaben

Dieser Abschnitt enthält Anweisungen zum Verwalten des WebNFS-Systems. Es folgen die relevanten Aufgaben.

TABELLE 5–4 Übersicht der Schritte für WebNFS-Systemverwaltungsaufgaben

Aufgabe	Beschreibung	Siehe
Plan für WebNFS	Faktoren, die zu berücksichtigen sind, bevor der WebNFS-Service aktiviert wird	„Planung für den WebNFS-Zugriff“ auf Seite 105
Aktivieren von WebNFS	Schritte zum Aktivieren des Einhängens eines NFS-Dateisystem mithilfe des WebNFS-Protokolls	„So aktivieren Sie den WebNFS-Zugang“ auf Seite 88
Aktivieren von WebNFS über eine Firewall	Schritte zum Ermöglichen des Zugriffs auf Dateien über eine Firewall mithilfe des WebNFS-Protokolls	„So aktivieren Sie den WebNFS-Zugriff über eine Firewall“ auf Seite 107
Suchen mithilfe einer NFS-URL	Anweisungen zum Verwenden einer NFS-URL innerhalb eines Webbrowsers	„So führen Sie Suchvorgänge mithilfe einer NFS-URL aus“ auf Seite 106
Verwenden einer Routine für den Zugriff auf öffentliche Dateien mit autofs	Schritte zum Erzwingen der Verwendung der Routine für den Zugriff auf öffentliche Dateien, wenn ein Dateisystem mit dem Automounter eingehängt wird	„So verwenden Sie eine Routine für den Zugriff auf öffentliche Dateien mit autofs“ auf Seite 121

TABELLE 5–4 Übersicht der Schritte für WebNFS-Systemverwaltungsaufgaben *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Verwenden einer NFS-URL mit autofs	Schritte zum Einfügen einer NFS-URL in die Automounter-Map	„So verwenden Sie die NFS-URLs mit autofs“ auf Seite 122
Ermöglichen des Zugriffs auf ein Dateisystem über eine Firewall	Schritte zur Zulassung des Zugriffs auf ein Dateisystem über eine Firewall mithilfe des WebNFS-Protokolls	„So hängen Sie ein NFS-Dateisystem über eine Firewall ein“ auf Seite 95
Einhängen eines Dateisystems mithilfe einer NFS-URL	Schritte zur Zulassung des Zugriffs auf ein Dateisystem mithilfe einer NFS-URL. Dieses Verfahren ermöglicht den Zugriff auf das Dateisystem ohne Verwendung des MOUNT-Protokolls.	„So hängen Sie ein NFS-Dateisystem mithilfe einer NFS-URL ein“ auf Seite 95

Planung für den WebNFS-Zugriff

Um WebNFS zu verwenden, müssen Sie zunächst eine Anwendung bereitstellen, die eine NFS-URL (beispielsweise `nfs://server/path`) ausführen und laden kann. Als Nächstes wird das Dateisystem ausgewählt, das für den WebNFS-Zugriff exportiert werden kann. Wenn die Anwendung Suchvorgänge im Web durchführt, wird oft das Dokument-Root-Verzeichnis für den Webserver verwendet. Bei der Auswahl eines Dateisystems, das für den WebNFS-Zugriff exportiert werden soll, sind verschiedene Faktoren zu berücksichtigen.

1. Jeder Server verfügt über eine Routine für den Zugriff auf öffentliche Dateien, die standardmäßig dem Root-Dateisystem des Servers zugewiesen ist. Der Pfad in einer NFS-URL wird in Relation zu dem Verzeichnis evaluiert, dem die Routine für den Zugriff auf öffentliche Dateien zugewiesen ist. Wenn der Pfad zu einer Datei oder einem Verzeichnis innerhalb eines exportierten Dateisystems führt, wird der Zugriff vom Server bereitgestellt. Sie können die Option `public` des Befehls `share` verwenden, um die Routine für den Zugriff auf öffentliche Dateien einem bestimmten exportierten Verzeichnis zuzuordnen. Mithilfe dieser Option werden URLs dem gemeinsam genutzten Dateisystem zugeordnet, nicht aber dem Root-Dateisystem des Servers. Das Root-Dateisystem lässt keinen Zugriff auf des Web zu, wenn es nicht gemeinsam genutzt wird.
2. Die WebNFS-Umgebung ermöglicht Benutzern, die bereits über Berechtigungen für das Einhängen verfügen, über einen Browser auf Dateien zuzugreifen. Diese Fähigkeit ist unabhängig davon vorhanden, ob es sich um ein Dateisystem handelt, das mithilfe der Option `public` exportiert wurde. Da die Benutzer bereits über NFS auf diese Dateien zugreifen können, sind mit dieser Art des Zugriffs keine weiteren Sicherheitsrisiken verbunden. Sie müssen ein Dateisystem nur dann mithilfe der Option `public` zur gemeinsamen Nutzung freigegeben werden, wenn Benutzer, die das Dateisystem nicht einhängen können, WebNFS-Zugriff benötigen.
3. Dateisysteme, die bereits öffentlich zur Verfügung stehen, eignen sich gut für die Verwendung der Option `public`. Dies gilt beispielsweise für das oberste Verzeichnis in einem FTP-Archiv oder das URL-Hauptverzeichnis einer Website.

4. Sie können die Option `index` zusammen mit dem Befehl `share` verwenden, um das Laden einer HTML-Datei zu erzwingen. Sie können das Verzeichnis aber auch auflisten, wenn auf eine NFS-URL zugegriffen wird.

   Nachdem ein Dateisystem ausgewählt ist, prüfen Sie die Dateien und legen die entsprechenden Zugriffsberechtigungen fest, um zu bestimmen, welche Dateien oder Verzeichnisse angezeigt werden dürfen. Legen Sie die entsprechenden Berechtigungen für jedes gemeinsam genutztes NFS-Dateisystem fest. Bei vielen Websites wird der Zugriff über `755`-Berechtigungen für Verzeichnisse und `644`-Berechtigungen für Dateien geregelt.

   Wenn sowohl NFS- als auch HTTP-URLs für den Zugriff auf eine Website verwendet werden, müssen Sie verschiedene weitere Faktoren berücksichtigen. Erläuterungen zu diesen Faktoren finden Sie unter „WebNFS-Beschränkungen bei Verwendung eines Webbrowsers“ auf Seite 208.

So führen Sie Suchvorgänge mithilfe einer NFS-URL aus

Browser, die den WebNFS-Service unterstützen, sollten Zugriff auf eine NFS-URL wie die folgende ermöglichen:

`nfs://`*server*`<:`*port*`>/`*path*

server	Name des Dateiservers
port	Portnummer, die zu verwenden ist (`2049`, Standardwert)
path	Pfad, der zu der betreffenden Datei führt und in Relation zur Routine für den Zugriff auf öffentliche Dateien oder zum Root-Dateisystem stehen kann

Hinweis – Bei den meisten Browsern wird der URL-Servicetyp (beispielsweise `nfs` oder `http`) von einer Transaktion zur nächsten beibehalten. Eine Ausnahme tritt ein, wenn eine URL geladen wird, die einen anderen Servicetyp enthält. Nachdem Sie eine NFS-URL verwendet haben, kann unter Umständen ein Verweis auf eine HTTP-URL geladen werden. Wenn ein solcher Verweis geladen wird, werden nachfolgende Seiten mithilfe des HTTP-Protokolls anstelle des NFS-Protokolls geladen.

So aktivieren Sie den WebNFS-Zugriff über eine Firewall

Sie können den WebNFS-Zugriff für Clients aktivieren, die nicht zum lokalen Teilnetz gehören, indem Sie die Firewall konfigurieren, um eine TCP-Verbindung an Port `2049` zuzulassen. Wenn der Zugriff für `httpd` zugelassen ist, bedeutet das nicht, dass NFS-URLs verwendet werden dürfen.

Aufgabenübersicht für die Autofs-Verwaltung

In diesem Abschnitt werden allgemeine Aufgaben beschrieben, die unter Umständen in Ihrer eigenen Umgebung ausgeführt werden müssen. Für jedes Szenario werden Verfahren zum Konfigurieren von autofs empfohlen, die bestens den Anforderungen Ihrer Clients genügen.

Hinweis – Ab Solaris 10 können Sie die `/etc/default/autofs`-Datei verwenden, um die autofs-Umgebung zu konfigurieren. Informationen zu Aufgaben finden Sie unter „Verwenden der `/etc/default/autofs` -Datei zum Konfigurieren Ihrer autofs-Umgebung“ auf Seite 109.

Übersicht der Schritte für die Autofs-Verwaltung

Die folgende Tabelle enthält Beschreibungen und Verweise auf viele Aufgaben, die mit autofs in Zusammenhang stehen.

TABELLE 5–5 Übersicht der Schritte für die Autofs-Verwaltung

Aufgabe	Beschreibung	Siehe
Starten von autofs	Starten des automount-Service, ohne das System neu zu starten	„So starten Sie den Automounter“ auf Seite 98
Stoppen von autofs	Stoppen des automount-Service, ohne andere Netzwerkdienste zu deaktivieren	„So stoppen Sie den Automounter“ auf Seite 98
Konfigurieren der autofs-Umgebung mithilfe der `/etc/default/autofs`-Datei	Zuweisen von Werten zu Schlüsselwörtern in der `/etc/default/autofs`-Datei	„Verwenden der `/etc/default/autofs` -Datei zum Konfigurieren Ihrer autofs-Umgebung“ auf Seite 109
Zugriff auf Dateisysteme mithilfe von autofs	Zugriff auf Dateisysteme mithilfe des automount-Service	„Einhängen mit dem Automounter“ auf Seite 92
Modifizieren der autofs-Maps	Schritte zum Modifizieren der Master-Map, die verwendet wird, um andere Maps aufzulisten	„So modifizieren Sie die Master-Map“ auf Seite 111

TABELLE 5–5 Übersicht der Schritte für die Autofs-Verwaltung *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
	Schritte zum Modifizieren einer indirekten Map, die für die meisten Maps verwendet wird	„So modifizieren Sie indirekte Maps“ auf Seite 112
	Schritte zum Modifizieren einer direkten Map, die verwendet wird, wenn eine direkte Zuordnung zwischen einem Einhängepunkt auf einem Client und einem Server erforderlich ist	„So modifizieren Sie direkte Maps“ auf Seite 112
Modifizieren der autofs-Maps, um auf Nicht-NFS-Dateisysteme zuzugreifen	Schritte zum Einrichten einer autofs-Map mit einem Eintrag für eine CD-ROM-Anwendung	„So greifen Sie mit autofs auf CD-ROM-Anwendungen zu“ auf Seite 113
	Schritte zum Einrichten einer autofs-Map mit einem Eintrag für eine PC-DOS-Diskette	„So greifen Sie mit autofs auf PC-DOS-Datendisketten zu“ auf Seite 114
	Schritte zum Verwenden von autofs, um auf ein CacheFS-Dateisystem zuzugreifen	„So greifen Sie mithilfe von CacheFS auf NFS-Dateisysteme zu“ auf Seite 115
Verwenden von `/home`	Beispiel für die Einrichtung einer allgemeinen `/home`-Map	„Einrichten einer allgemeinen Ansicht von `/home`“ auf Seite 116
	Schritte zum Einrichten einer `/home`-Map, die sich auf mehrere Dateisysteme bezieht	„So richten Sie `/home` mit mehreren Home-Verzeichnis-Dateisystemen ein“ auf Seite 116
Verwenden eines neuen autofs-Einhängepunkts	Schritte zum Einrichten einer projektbezogenen autofs-Map	„So konsolidieren Sie projektbezogene Dateien unter `/ws`“ auf Seite 117
	Schritte zum Einrichten einer autofs-Map, die verschiedene Clientarchitekturen unterstützt	„So richten Sie verschiedene Architekturen ein, um auf einen gemeinsam genutzten Namespace zuzugreifen“ auf Seite 119
	Schritte zum Einrichten einer autofs-Map, die verschiedene Betriebssysteme unterstützt	„So unterstützen Sie nicht kompatible Client-Betriebssystemversionen“ auf Seite 120
Replizieren von Dateisystemen mit autofs	Ermöglichen des Zugriffs auf Dateisysteme, bei denen ein Failover stattfindet	„So replizieren Sie gemeinsam genutzte Dateien auf mehreren Servern“ auf Seite 120
Verwenden von Sicherheitsbeschränkungen mit autofs	Ermöglichen des Zugriffs auf Dateisysteme bei gleichzeitiger Beschränkung des Remote-`Root`-Zugriffs auf die Dateien	„So wenden Sie Autofs-Sicherheitsbeschränkungen an“ auf Seite 121
Verwenden einer Routine für den Zugriff auf öffentliche Dateien mit autofs	Erzwingen der Verwendung der Routine für den Zugriff auf öffentliche Dateien beim Einhängen eines Dateisystems	„So verwenden Sie eine Routine für den Zugriff auf öffentliche Dateien mit autofs“ auf Seite 121

TABELLE 5–5 Übersicht der Schritte für die Autofs-Verwaltung *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Verwenden einer NFS-URL mit autofs	Einfügen einer NFS-URL, damit diese vom Automounter verwendet werden kann	„So verwenden Sie die NFS-URLs mit autofs“ auf Seite 122
Deaktivieren der autofs-Durchsuchfunktion	Schritte zum Deaktivieren der Durchsuchfunktion, damit die autofs-Einhängepunkte nicht automatisch auf einem einzelnen Client belegt werden	„So deaktivieren Sie vollständig die autofs-Durchsuchfunktion auf einem einzelnen NFS-Client“ auf Seite 123
	Schritte zum Deaktivieren der Durchsuchfunktion, damit die autofs-Einhängepunkte nicht automatisch auf allen Clients belegt werden	„So deaktivieren Sie die autofs-Durchsuchfunktion aller Clients“ auf Seite 123
	Schritte zum Deaktivieren der Durchsuchfunktion, damit ein bestimmter autofs-Einhängepunkt nicht automatisch auf einem Client belegt wird	„So deaktivieren Sie die autofs-Durchsuchfunktion auf einem ausgewählten Dateisystem“ auf Seite 124

Verwenden der `/etc/default/autofs` -Datei zum Konfigurieren Ihrer autofs-Umgebung

Ab Solaris 10 können Sie die `/etc/default/autofs`-Datei verwenden, um Ihre autofs-Umgebung zu konfigurieren. Mit dieser Datei steht jetzt eine weitere Möglichkeit zum Konfigurieren der autofs-Befehle und autofs-Dämonen zur Verfügung. Dieselben Angaben, die Sie normalerweise über die Befehlszeile eingeben, können jetzt in diese Konfigurationsdatei eingetragen werden. Sie können die erforderlichen Angaben machen, indem Sie Werte für Schlüsselwörter verwenden. Weitere Informationen finden Sie unter „`/etc/default/autofs`-Datei“ auf Seite 143.

Das folgende Verfahren zeigt, wie die `/etc/default/autofs` -Datei verwendet wird.

▼ Konfigurieren der autofs-Umgebung mithilfe der `/etc/default/autofs`-Datei

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie einen Eintrag in die `/etc/default/autofs`-Datei ein, oder ändern Sie einen Eintrag in dieser Datei.**

Um beispielsweise die Durchsuchfunktion für alle autofs-Einhängepunkte zu deaktivieren, fügen Sie die folgende Zeile ein:

```
AUTOMOUNTD_NOBROWSE=ON
```

Dieses Schlüsselwort entspricht dem Argument `-n` für `automountd`. Eine Liste der Schlüsselwörter finden Sie unter „`/etc/default/autofs`-Datei“ auf Seite 143.

3 **Starten Sie den autofs-Dämon neu.**

Geben Sie folgenden Befehl ein:

```
# svcadm restart system/filesystem/autofs
```

Aufgaben zur Verwaltung von Maps

In der folgenden Tabelle werden verschiedene Faktoren aufgeführt, die Sie beim Verwalten von autofs-Maps berücksichtigen müssen. Die von Ihnen gewählte Map und der Name Service beeinflussen den Mechanismus, den Sie benötigen, um Änderungen an den autofs-Maps vorzunehmen.

In der folgenden Tabelle werden die Arten von Maps und deren Verwendung beschrieben.

TABELLE 5–6 Arten und Verwendung von autofs-Maps

Art der Map	Verwendung
Master	Ordnet ein Verzeichnis mit einer Map zu.
Direkt	Ordnet autofs bestimmten Dateisystemen zu.
Indirekt	Ordnet autofs referenzorientierten Dateisystemen zu.

In der folgenden Tabelle wird beschrieben, wie Sie entsprechend Ihrem Name Service Änderungen an Ihrer autofs-Umgebung vornehmen.

TABELLE 5–7 Pflege von Maps

Name Service	Methode
Lokale Dateien	Texteditor
NIS	`make`-Dateien
NIS+	`nistbladm`

In der folgenden Tabelle erfahren Sie, wann der Befehl `automount` auszuführen ist, was von den Änderungen abhängt, die Sie an der Map vorgenommen haben. Wenn Sie beispielsweise einen Zusatz in eine direkte Map eingetragen oder eine Löschung vorgenommen haben, müssen Sie auf dem lokalen System den Befehl `automount` ausführen. Sobald der Befehl ausgeführt ist, wird die Änderung wirksam. Wenn Sie jedoch einen bestehenden Eintrag modifiziert haben, ist es nicht nötig, den Befehl `automount` auszuführen, damit die Änderung wirksam wird.

TABELLE 5–8 Wann der Befehl `automount` auszuführen ist

Art der Map	`automount` neu starten?	
	Zusatz oder Löschung	Änderung
`auto_master`	J	J
`direct`	J	N
`indirect`	N	N

Modifizieren der Maps

Für den folgenden Vorgang ist NIS+ als Ihr Name Service erforderlich.

▼ So modifizieren Sie die Master-Map

1. **Melden Sie sich als ein Benutzer an, der über Berechtigungen zum Ändern der Maps verfügt.**
2. **Verwenden Sie den Befehl `nistbladm`, um die Master-Map zu ändern.**

   Lesen Sie dazu *System Administration Guide: Naming and Directory Services (NIS+)* .
3. **Melden Sie sich für jeden Client als Superuser oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.
4. **Führen Sie für jeden Client den Befehl `automount` aus, um sicherzustellen, dass Ihre Änderungen wirksam werden.**
5. **Setzen Sie Ihre Benutzer von den Änderungen in Kenntnis.**

   Dies ist notwendig, damit die Benutzer den Befehl `automount` als Superuser auf ihren eigenen Rechnern ausführen können. Immer, wenn der Befehl `automount` ausgeführt wird, werden Informationen aus der Master-Map gesammelt.

▼ So modifizieren Sie indirekte Maps

1. **Melden Sie sich als ein Benutzer an, der über Berechtigungen zum Ändern der Maps verfügt.**
2. **Verwenden Sie den Befehl `nistbladm`, um Änderungen an der indirekten Map vorzunehmen.**

   Lesen Sie dazu *System Administration Guide: Naming and Directory Services (NIS+)* . Beachten Sie, dass die Änderungen erst dann wirksam werden, wenn die Map das nächste Mal verwendet wird, d. h. beim nächsten Einhängevorgang.

▼ So modifizieren Sie direkte Maps

1. **Melden Sie sich als ein Benutzer an, der über Berechtigungen zum Ändern der Maps verfügt.**
2. **Verwenden Sie den Befehl `nistbladm`, um Änderungen an der direkten Map vorzunehmen oder Änderungen aus der direkten Map zu entfernen.**

   Lesen Sie dazu *System Administration Guide: Naming and Directory Services (NIS+)* .
3. **Setzen Sie Ihre Benutzer von den Änderungen in Kenntnis.**

   Dies ist notwendig, damit die Benutzer den Befehl `automount` als Superuser auf ihren eigenen Rechnern ausführen können.

Hinweis – Wenn Sie nur den Inhalt eines Eintrags in einer direkten Map ändern, ist es nicht nötig, den Befehl `automount` auszuführen.

Beispiel: Sie modifizieren die `auto_direct`-Map, wodurch das `/usr/src`-Verzeichnis von einem anderen Server eingehängt wird. Wenn `/usr/src` nicht zu diesem Zeitpunkt eingehängt wird, wird der neue Eintrag wirksam, sobald Sie versuchen, auf `/usr/src` zuzugreifen. Sobald `/usr/src` eingehängt ist, können Sie warten, bis das automatische Aushängen stattfindet, und dann auf die Datei zugreifen.

Hinweis – Verwenden Sie indirekte Maps sooft wie möglich. Indirekte Maps können einfacher erstellt werden und stellen weniger Ansprüche an die Dateisysteme des Rechners. Auch nehmen indirekte Maps weniger Speicherplatz in der Einhängetabelle als direkte Maps ein.

Vermeiden von Einhängepunktkonflikten

Wenn Sie über ein lokale Datenträgerpartition verfügen, die auf `/src` eingehängt ist, und beabsichtigen, den autofs-Service zum Einhängen der anderen Quellverzeichnisse zu

verwenden, sehen Sie sich möglicherweise mit einem Problem konfrontiert. Wenn Sie den Einhängepunkt `/src` angeben, blendet der NFS-Service die lokale Partition immer dann aus, wenn Sie versuchen, darauf zuzugreifen.

Sie müssen die Partition an einer anderen Stelle einhängen, beispielsweise `/export/src`. Dann benötigen Sie in `/etc/vfstab` einen Eintrag wie den folgenden:

```
/dev/dsk/d0t3d0s5 /dev/rdsk/c0t3d0s5 /export/src ufs 3 yes -
```

Auch benötigen Sie diesen Eintrag in `auto_src`:

```
terra        terra:/export/src
```

`terra` ist der Name des Rechners.

Zugreifen auf Nicht-NFS-Dateisysteme

Autofs kann auch andere Dateien als NFS-Dateien einhängen. Autofs hängt Dateien auf Wechseldatenträgern ein, beispielsweise Disketten oder CD-ROMs. Normalerweise hängen Sie Dateien mithilfe des Volume Manager auf Wechseldatenträgern ein. Das folgende Beispiel zeigt, wie dieser Vorgang mithilfe von autofs ausgeführt werden kann. Der Volume Manager und autofs arbeiten nicht zusammen. Aus diesem Grund muss der Volume Manager zunächst deaktiviert werden, damit die betreffenden Einträge verwendet werden können.

Anstatt ein Dateisystem von einem Server einzuhängen, legen Sie den betreffenden Datenträger in das Laufwerk ein und stellen über die Map einen Verweis auf das Dateisystem her. Wenn Sie autofs verwenden und beabsichtigen, auf Nicht-NFS-Dateisysteme zuzugreifen, gehen Sie zu den nachstehenden Verfahren über.

▼ So greifen Sie mit autofs auf CD-ROM-Anwendungen zu

Hinweis – Wenden Sie dieses Verfahren an, wenn Sie Volumen Manager *nicht* verwenden.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Aktualisieren Sie die autofs-Map.

Fügen Sie einen Eintrag wie den folgenden für das CD-ROM-Dateisystem ein:

```
hsfs      -fstype=hsfs,ro      :/dev/sr0
```

Der Name des CD-ROM-Geräts, das eingehängt werden soll, muss hinter dem Doppelpunkt stehen.

▼ So greifen Sie mit autofs auf PC-DOS-Datendisketten zu

Hinweis – Wenden Sie dieses Verfahren an, wenn Sie Volumen Manager *nicht* verwenden.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Aktualisieren Sie die autofs-Map.**

Fügen Sie einen Eintrag wie den folgenden für das Diskettendateisystem ein:

```
pcfs     -fstype=pcfs     :/dev/diskette
```

Zugreifen auf NFS-Dateisysteme mithilfe von CacheFS

Das Cache-Dateisystem (CacheFS) ist ein generischer Mechanismus für die dauerhafte Zwischenspeicherung. CacheFS stützt sich auf eine kleine, schnelle lokale Festplatte und trägt so zur Leistungssteigerung bestimmter Dateisysteme bei. Mit CacheFS lässt sich beispielsweise die Leistung der NFS-Umgebung verbessern.

Dabei hängt die Funktionsweise von CacheFS von der jeweiligen NFS-Version ab. Wenn beispielsweise sowohl auf dem Client als auch im Back-Dateisystem NFS Version 2 oder Version 3 ausgeführt wird, werden die Dateien für den Zugriff durch den Client im Front-Dateisystem zwischengespeichert. Wird jedoch sowohl auf dem Client als auch auf dem Server NFS Version 4 ausgeführt, gilt folgende Funktionsweise: Wenn der Client die erste Zugriffsanforderung für eine Datei aus einem CacheFS-Dateisystem ausgibt, umgeht diese Anforderung das Front- bzw. Cache-Dateisystem und erreicht direkt das Back-Dateisystem. Mit NFS Version 4 werden Dateien nicht mehr in einem Front-Dateisystem zwischengespeichert. Der gesamte Dateizugriff erfolgt über das Back-Dateisystem. Da keine Zwischenspeicherung von Dateien im Front-Dateisystem stattfindet, werden CacheFS-spezifische Einhängeoptionen ignoriert, die für das Front-Dateisystem bestimmt sind. CacheFS-speizifische Einhängeoptionen gelten nicht für das Back-Dateisystem.

Hinweis – Wenn Sie Ihr System erstmals für NFS Version 4 konfigurieren, wird auf der Konsole der Warnhinweis angezeigt, dass keine Zwischenspeicherung mehr stattfindet.

▼ So greifen Sie mithilfe von CacheFS auf NFS-Dateisysteme zu

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Führen Sie den Befehl `cfsadmin` aus, um ein Cache-Verzeichnis auf der lokalen Festplatte zu erstellen.**

```
# cfsadmin -c /var/cache
```

3 **Fügen Sie den `cachefs`-Eintrag in die entsprechende Automounter-Map ein.**

Wenn beispielsweise der folgende Eintrag in die Master-Map eingefügt wird, werden alle Home-Verzeichnisse im Cache gespeichert:

```
/home auto_home -fstype=cachefs,cachedir=/var/cache,backfstype=nfs
```

Wenn der folgende Eintrag in die `auto_home`-Map eingefügt wird, wird nur das Home-Verzeichnis des Benutzers `rich` im Cache gespeichert:

```
rich -fstype=cachefs,cachedir=/var/cache,backfstype=nfs dragon:/export/home1/rich
```

Hinweis – Optionen, die in Maps enthalten sind, die zu einem späteren Zeitpunkt durchsucht werden, setzen Optionen außer Kraft, die in Maps enthalten sind, die zu einem früheren Zeitpunkt durchsucht werden. Die zuletzt gefundenen Optionen werden verwendet. Im vorangegangenen Beispiel muss ein zusätzlicher Eintrag in der `auto_home`-Map nur die Optionen in der Master-Map enthalten, wenn aufgrund mancher Optionen Änderungen erforderlich waren.

Anpassen des Automounters

Zum Einrichten der Automounter-Maps stehen viele Möglichkeiten zur Verfügung. Die folgenden Aufgaben zeigen, wie die Automounter-Maps angepasst werden können, um die Handhabung der Verzeichnisstruktur zu vereinfachen.

Einrichten einer allgemeinen Ansicht von /home

Alle Netzwerkbenutzer sollten ihr eigenes Home-Verzeichnis oder das Home-Verzeichnis anderer Benutzer unter /home lokalisieren können. Diese Ansicht sollte auf jedem Rechner – egal ob Client oder Server – vorhanden sein.

Jede Solaris-Installation verfügt über eine Master-Map: /etc/auto_master.

```
# Master map for autofs
#
+auto_master
/net     -hosts     -nosuid,nobrowse
/home    auto_home  -nobrowse
```

Eine Map für auto_home ist zudem unter /etc installiert.

```
# Home directory map for autofs
#
+auto_home
```

Abgesehen von einem Verweis auf eine externe auto_home-Map ist diese Map leer. Wenn die Verzeichnisse unter /home für alle anderen Rechner verfügbar sein sollen, darf die /etc/auto_home-Map nicht geändert werden. Alle Verzeichniseinträge müssen in den Name Service-Dateien stehen, entweder NIS oder NIS+.

Hinweis – Den Benutzern sollte nicht erlaubt sein, ausführbare setuid-Dateien aus ihren Home-Verzeichnissen auszuführen. Ohne diese Beschränkung würde jeder Benutzer über Superuser-Berechtigungen für jeden Rechner verfügen können.

▼ So richten Sie /home mit mehreren Home-Verzeichnis-Dateisystemen ein

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Installieren Sie Home-Verzeichnispartitionen unter /export/home.**

   Wenn das System mehrere Partitionen hat, installieren Sie die Partitionen in verschiedenen Verzeichnissen, beispielsweise /export/home1 und /export/home2.

3 Verwenden Sie die Tools der Solaris Management Console, um die `auto_home`-Map zu erstellen und zu verwalten.

Wenn Sie ein neues Benutzerkonto erstellen, geben Sie den Speicherort des Home-Verzeichnisses des Benutzers in der `auto_home`-Map an. Map-Einträge können einfach sein, zum Beispiel:

```
rusty        dragon:/export/home1/&
gwenda       dragon:/export/home1/&
charles      sundog:/export/home2/&
rich         dragon:/export/home3/&
```

Beachten Sie, dass das Und-Zeichen (&) den Schlüssel der Map ersetzt. Das Und-Zeichen ist eine Abkürzung für das zweite Auftreten von `rusty` im folgenden Beispiel:

```
rusty         dragon:/export/home1/rusty
```

Wenn die `auto_home`-Map vorhanden ist, können Benutzer mit dem Pfad `/home/` *user* auf jedes Home-Verzeichnis (einschließlich das eigene) verweisen. *user* ist der Anmeldename der Benutzer und der Schlüssel in der Map. Diese allgemeine Ansicht aller Home-Verzeichnisse ist für die Anmeldung beim Rechner eines anderen Benutzers hilfreich. Autofs hängt Ihr Home-Verzeichnis für Sie ein. Im Clientprogramm wird dieselbe Ansicht des `/home`-Verzeichnisses angezeigt, wenn Sie einen Remote-Fenstersystemclient auf einem anderen Rechner ausführen.

Diese allgemeine Ansicht schließt auch den Server ein. Um beim vorangegangenen Beispiel zu bleiben: Wenn `rusty` sich beim Server `dragon` anmeldet, bietet autofs dort direkten Zugriff auf die lokale Festplatte, indem `/export/home1/rusty` über eine Schleife auf `/home/rusty` eingehängt wird.

Benutzer müssen nicht den wirklichen Speicherort Ihrer Home-Verzeichnisse kennen. Wenn `rusty` mehr Speicherplatz benötigt und sein Home-Verzeichnis auf einen anderen Server verlegt werden muss, reicht eine einfache Änderung nicht aus. Sie müssen dann den Eintrag von `rusty` in der `auto_home`-Map ändern, um den neuen Speicherort zu reflektieren. Andere Benutzer können weiterhin den `/home/rusty` -Pfad verwenden.

▼ So konsolidieren Sie projektbezogene Dateien unter `/ws`

Angenommen, Sie sind der Administrator eines großen Softwareentwicklungsprojekts. Sie beabsichtigen, alle projektbezogenen Dateien in einem Verzeichnis namens `/ws` zur Verfügung zu stellen. Auf dieses Verzeichnis soll von allen Workstations aus zugegriffen werden können.

1 Fügen Sie einen Eintrag für das Verzeichnis `/ws` in die `auto_master`-Map ein, entweder NIS oder NIS+.

```
/ws     auto_ws     -nosuid
```

Anhand der `auto_ws`-Map werden die Inhalte des `/ws`-Verzeichnisses definiert.

2 Fügen Sie aus Sicherheitsgründen die Option `-nosuid` ein.

Diese Option verhindert, dass Benutzer setuid-Programme ausführen, die in jedem Arbeitsbereich vorhanden sein können.

3 Fügen Sie die Einträge in die `auto_ws`-Map ein.

Die `auto_ws`-Map ist so aufgebaut, dass jeder Eintrag ein Unterprojekt beschreibt. Nach Ihrem ersten Versuch erhalten Sie eine Map, die wie folgt aussieht:

```
compiler   alpha:/export/ws/&
windows    alpha:/export/ws/&
files      bravo:/export/ws/&
drivers    alpha:/export/ws/&
man        bravo:/export/ws/&
tools      delta:/export/ws/&
```

Das am Ende jedes Eintrags stehende Und-Zeichen (&) ist eine Abkürzung des Eintragsschlüssels. Der erste Eintrag entspricht beispielsweise Folgendem:

```
compiler        alpha:/export/ws/compiler
```

Das Ergebnis Ihres ersten Versuchs ist eine einfache, aber ungeeignete Map. Der Projektleiter beschließt, dass die Dokumentation im `man`-Eintrag als Unterverzeichnis unter jedem Unterprojekt zur Verfügung stehen soll. Jedes Unterprojekt erfordert Unterverzeichnisse zum Beschreiben der verschiedenen Softwareversionen. Jedes dieser Unterverzeichnisse muss einer vollständigen Festplattenpartition auf dem Server zugewiesen werden.

Modifizieren Sie die Einträge in der Map wie folgt:

```
compiler \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /vers2.0    bravo:/export/ws/&/vers2.0 \
    /man        bravo:/export/ws/&/man
windows \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /man        bravo:/export/ws/&/man
files \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /vers2.0    bravo:/export/ws/&/vers2.0 \
    /vers3.0    bravo:/export/ws/&/vers3.0 \
    /man        bravo:/export/ws/&/man
drivers \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /man        bravo:/export/ws/&/man
tools \
    /           delta:/export/ws/&
```

Obwohl die Map jetzt viel größer erscheint, enthält sie nur fünf Einträge. Jeder Eintrag ist größer, weil mehrere Einhängepunkte enthalten sind. Beispielsweise erfordert ein Verweis auf `/ws/compiler` drei Einhängepunkte für die Verzeichnisse `vers1.0`, `vers2.0` und `man`. Der umgekehrte Schrägstrich am Ende jeder Zeile informiert autofs, dass der Eintrag auf der nächsten Zeile weitergeht. Der Eintrag befindet sich in einer langen Zeile, obwohl die Lesbarkeit des Eintrags durch Zeilenumbrüche und Einrückungen verbessert wurde. Das

Verzeichnis `tools` enthält Softwareentwicklungtools für alle Unterprojekte, wodurch dieses Verzeichnis nicht von derselben Unterverzeichnisstruktur abhängig ist. Das Verzeichnis `tools` ist weiterhin ein einzelner Einhängepunkt.

Dadurch erhält der Administrator viel Flexibilität. Softwareprojekte erfordern normalerweise viel Festplattenspeicher. Während der Umsetzung des Projekts kann es nötig sein, verschiedene Festplattenpartitionen zu verschieben und zu erweitern. Wenn diese Änderungen in der `auto_ws`-Map reflektiert werden, müssen die Benutzer nicht benachrichtigt werden, da die Verzeichnishierarchie unter `/ws` unverändert bleibt.

Da die Server `alpha` und `bravo` dieselbe autofs-Map anzeigen, können Benutzer, die sich bei diesen Rechnern anmelden, wie erwartet auf den `/ws`-Namespace zugreifen. Diese Benutzer haben über Schleifeneinhängepunkte anstelle von NFS-Einhängepunkten direkten Zugriff auf lokale Dateien.

▼ So richten Sie verschiedene Architekturen ein, um auf einen gemeinsam genutzten Namespace zuzugreifen

Sie müssen einen gemeinsam genutzten Namespace für lokale ausführbare Dateien und Anwendungen wie beispielsweise Tabellenkalkulations- und Textverarbeitungsanwendungen einrichten. Die Clients dieses Namespace verwenden verschiedene Workstation-Architekturen, die verschiedene ausführbare Formate erfordern. Außerdem führen manche Workstations verschiedene Betriebssystemversionen aus.

1. **Erstellen Sie die `auto_local`-Map.**

   Lesen Sie dazu *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*.

2. **Wählen Sie einen eindeutigen, standortspezifischen Namen für den gemeinsam genutzten Namespace.**

   Dadurch können die zu diesem Namespace gehörenden Dateien und Verzeichnisse einfach identifiziert werden. Wenn Sie beispielsweise den Namen `/usr/local` wählen, ist der Pfad `/usr/local/bin` ein Teil dieses Namespace.

3. **Erstellen Sie zur Gewährleistung einer einfachen Erkennbarkeit für den Benutzer eine indirekte autofs-Map.**

   Hängen Sie diese Map in `/usr/local` ein. Richten Sie den folgenden Eintrag in der NIS-`auto_master`-Map ein:

   ```
   /usr/local     auto_local     -ro
   ```

   Die die Einhängeoption `-ro` bedeutet, dass Clients keine Dateien oder Verzeichnisse beschreiben können.

4. **Exportieren Sie das entsprechende Verzeichnis auf dem Server.**

5 **Fügen Sie einen `bin`-Eintrag in die auto_local-Map ein.**

Die Struktur Ihres Verzeichnisses hat folgendes Aussehen:

```
bin      aa:/export/local/bin
```

6 **(Optional) Um Clients von verschiedenen Architekturen zu bedienen, ändern Sie den Eintrag, indem Sie die autofs-Variable `CPU` hinzufügen.**

```
bin      aa:/export/local/bin/$CPU
```

- Für SPARC-Clients – fügen Sie ausführbare Dateien in `/export/local/bin/sparc` ein.
- Für x86-Clients – fügen Sie ausführbare Dateien in `/export/local/bin/i386` ein.

▼ So unterstützen Sie nicht kompatible Client-Betriebssystemversionen

1 **Kombinieren Sie den Architekturtyp mit einer Variablen, die den Betriebssystemtyp des Clients bestimmt.**

Sie können die autofs-Variable `OSREL` mit der Variable `CPU` kombinieren, um einen Namen zu bilden, der sowohl den CPU-Typ als auch die Betriebssystemversion bestimmt.

2 **Erstellen Sie den folgenden Map-Eintrag:**

```
bin      aa:/export/local/bin/$CPU$OSREL
```

Für Clients, auf denen die Version 5.6 des Betriebssystems ausgeführt wird, exportieren Sie die folgenden Dateisysteme:

- Für SPARC-Clients – exportieren Sie `/export/local/bin/sparc5.6` .
- Für x86-Clients – fügen Sie ausführbare Dateien in `/export/local/bin/i3865.6` ein.

▼ So replizieren Sie gemeinsam genutzte Dateien auf mehreren Servern

Die beste Methode zur Festlegung der gemeinsamen Nutzung replizierter schreibgeschützter Dateisysteme ist die Verwendung eines Failover. Eine Erläuterung des Failover finden Sie unter „Clientseitiges Failover“ auf Seite 202.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Modifizieren Sie den Eintrag in den autofs-Maps.**

Erstellen Sie eine durch Komma getrennte Liste aller Replikatserver wie die folgende:

```
bin     aa,bb,cc,dd:/export/local/bin/$CPU
```

Autofs wählt den nächsten Server aus. Wenn ein Server mehrere Netzwerkschnittstellen hat, listen Sie jede Schnittstelle auf. Autofs wählt die Schnittstelle, die dem Client am nächsten liegt, wodurch unnötiges Routing des NFS-Verkehrs vermieden wird.

▼ So wenden Sie Autofs-Sicherheitsbeschränkungen an

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Erstellen Sie den folgenden Eintrag in der Name Service-`auto_master`-Datei, entweder NIS oder NIS+:**

```
/home     auto_home     -nosuid
```

Die Option `nosuid` verhindert, das Benutzer mit dem `setuid`- oder `setgid`-Bitsatz Dateien erstellen.

Dieser Eintrag setzt den Eintrag für `/home` in einer generischen lokalen `/etc/auto_master`-Datei außer Kraft. Siehe vorangegangenes Beispiel. Der Eintrag wird außer Kraft gesetzt, weil der `+auto_master`-Verweis auf die Map des externen Name Service vor dem `/home`-Eintrag in der Datei steht. Wenn die Einträge in der `auto_home`-Map Einhängeoptionen enthalten, wird die Option `nosuid` überschrieben. Aus diesem Grund dürfen entweder keine Optionen in der `auto_home`-Map verwendet werden, oder die Option `nosuid` muss in jedem Eintrag enthalten sein.

Hinweis – Hängen Sie die Festplattenpartitionen des Home-Verzeichnisses weder im oder unter `/home` auf dem Server ein.

▼ So verwenden Sie eine Routine für den Zugriff auf öffentliche Dateien mit autofs

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Erstellen Sie einen Eintrag in der autofs-Map wie den folgenden:**

```
/usr/local     -ro,public    bee:/export/share/local
```

Mit der Option `public` wird die Verwendung der Routine für den Zugriff auf öffentliche Dateien erzwungen. Wenn der NFS-Server keine Routinen den für Zugriff auf öffentliche Dateien unterstützt, schlägt das Einhängen fehl.

▼ So verwenden Sie die NFS-URLs mit autofs

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Erstellen Sie einen autofs-Eintrag wie den folgenden:**

```
/usr/local     -ro    nfs://bee/export/share/local
```

Der Service versucht, die Routine für den Zugriff auf öffentliche Dateien auf dem NFS-Server zu verwenden. Wenn der NFS-Server jedoch keine Routinen für den Zugriff auf öffentliche Dateien unterstützt, wird das MOUNT-Protokoll verwendet.

Deaktivieren der autofs-Durchsuchfunktion

In der installierten Standardversion von `/etc/auto_master` ist die Option `-nobrowse` für die Einträge in `/home` und `/net` enthalten. Außerdem wird durch das Upgrade die Option `-nobrowse` zu den `/home`- und `/net`-Einträgen in `/etc/auto_master` hinzugefügt, wenn diese Einträge nicht modifiziert wurden. Jedoch müssen Sie diese Änderungen manuell vornehmen oder nach der Installation die Durchsuchfunktion für standortspezifische autofs-Einhängepunkte deaktivieren.

Es gibt viele Möglichkeiten, die Durchsuchfunktion zu deaktivieren. Deaktivieren Sie die Funktion mithilfe einer Befehlszeilenoption für den `automountd`-Dämon, wodurch die autofs-Durchsuchfunktion des Clients komplett deaktiviert wird. Sie haben auch die Möglichkeit, die Durchsuchfunktion für jeden Map-Eintrag auf allen Clients zu deaktivieren, indem Sie die autofs-Maps in einem NIS- oder NIS+-Namespace verwenden. Darüber hinaus können Sie die Funktion für jeden Map-Eintrag auf jedem Client deaktivieren, indem Sie lokale autofs-Maps verwenden, wenn kein netzwerkübergreifender Namespace verwendet wird.

So deaktivieren Sie vollständig die autofs-Durchsuchfunktion auf einem einzelnen NFS-Client

1. **Melden Sie sich als Superuser oder als Benutzer mit einer entsprechenden Rolle beim NFS-Client an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Bearbeiten Sie die `/etc/default/autofs`-Datei, um das folgende Schlüsselwort und den folgenden Wert einzugeben:**

   ```
   AUTOMOUNTD_NOBROWSE=TRUE
   ```

3. **Starten Sie den autofs-Service neu.**

   ```
   # svcadm restart system/filesystem/autofs
   ```

So deaktivieren Sie die autofs-Durchsuchfunktion aller Clients

Um die Durchsuchfunktion aller Clients zu deaktivieren, müssen Sie einen Name Service wie NIS oder NIS+ verwenden. Anderenfalls müssen Sie die Automounter-Maps auf jedem Client manuell bearbeiten. In diesem Beispiel ist die Durchsuchfunktion des `/home`-Verzeichnisses deaktiviert. Wenden Sie dieses Verfahren bei jedem indirekten autofs-Knoten an, der deaktiviert werden soll.

1. **Fügen Sie die Option `-nobrowse` in den `/home`-Eintrag in der `auto_master`-Datei des Name Service ein.**

   ```
   /home     auto_home     -nobrowse
   ```

2. **Führen Sie den Befehl `automount` auf allen Clients aus.**

   Das neue Verhalten wird wirksam, nachdem Sie den Befehl `automount` auf den Clientsystemen ausgeführt oder das System neu gestartet haben.

   ```
   # /usr/sbin/automount
   ```

▼ So deaktivieren Sie die autofs-Durchsuchfunktion auf einem ausgewählten Dateisystem

In diesem Beispiel wird gezeigt, wie die Durchsuchfunktion des `/net`-Verzeichnisses deaktiviert wird. Sie können dasselbe Verfahren für `/home` oder andere autofs-Einhängepunkte verwenden.

1 Prüfen Sie den `automount`-Eintrag in `/etc/nsswitch.conf`.

Damit lokale Dateieinträge Vorrang haben, müssen die Dateien des Eintrags in der Name Service Switch-Datei vor dem Name Service aufgelistet sein. Beispiel:

```
automount:  files nis
```

Dieser Eintrag zeigt die Standardkonfiguration in einer standardmäßigen Solaris-Installation.

2 Prüfen Sie die Position des `+auto_master` -Eintrags in `/etc/auto_master`.

Damit zusätzliche Einträge in den lokalen Dateien Vorrang vor den Einträgen im Namespace haben, muss der `+auto_master`-Eintrag verschoben werden, sodass er hinter `/net` steht:

```
# Master map for automounter
#
/net    -hosts     -nosuid
/home   auto_home
/xfn    -xfn
+auto_master
```

In einer Standardkonfiguration steht der `+auto_master`-Eintrag am Anfang der Datei. Dadurch wird verhindert, dass lokale Änderungen verwendet werden.

3 Fügen Sie die Option `nobrowse` in den `/net`-Eintrag in der `/etc/auto_master`-Datei ein.

```
/net     -hosts     -nosuid,nobrowse
```

4 Führen Sie auf allen Clients den Befehl `automount` aus.

Das neue Verhalten wird wirksam, nachdem Sie den Befehl `automount` auf den Clientsystemen ausgeführt oder das System neu gestartet haben.

```
# /usr/sbin/automount
```

Strategien für die NFS-Fehlerbehebung

Beim Verfolgen eines NFS-Problems sollten Sie die wichtigsten möglichen Ausfallpunkte berücksichtigen: Server, Client und Netzwerk. Anhand der in diesem Abschnitt erläuterten Strategie wird versucht, einzelne Komponenten zu isolieren, um festzustellen, welche dieser Komponenten nicht funktioniert. In allen Fällen müssen die `mountd`- und `nfsd`-Dämonen auf dem Server ausgeführt werden, damit Remote-Einhängevorgänge erfolgreich durchgeführt werden können.

Die Option `-intr` ist standardmäßig für alle Einhängepunkte aktiviert. Wenn ein Programm hängengeblieben ist und die Meldung `server not responding` (Server antwortet nicht) angezeigt wird, können Sie das Programm mit dem Tastaturbefehl Strg-c abbrechen.

Wenn das Netzwerk oder der Server von Problemen betroffen sind, machen sich Ausfälle von Programmen, die auf hart eingehängte Remote-Dateien zugreifen, anders bemerkbar als Ausfälle von Programmen, die auf weich eingehängte Remote-Dateien zugreifen. Hart eingehängte Remote-Dateisysteme bewirken, dass der Kernel des Clients so lange versucht, die betreffenden Abfragen durchzuführen, bis der Server wieder antwortet. Weich eingehängte Remote-Dateisysteme bewirken, dass nach einigen Abfrageversuchen des Clients eine Fehlermeldung zurückgegeben wird. Da diese Fehler zu unerwarteten Anwendungsfehlern und Datenbeschädigungen führen können, sollten weiche Einhängevorgänge vermieden werden.

Bei einem hart eingehängten Dateisystem bleibt ein Programm, das versucht, auf das Dateisystem zuzugreifen, hängen, wenn der Server nicht antwortet. In diesem Fall wird auf der Konsole folgende Meldung angezeigt:

```
NFS server hostname not responding still trying
```

Wenn der Server schließlich antwortet, wird folgende Meldung angezeigt:

```
NFS server hostname ok
```

Bei einem Programm, das auf ein weich eingehängtes Dateisystem zugreift, dessen Server nicht antwortet, wird die folgende Meldung angezeigt:

```
NFS operation failed for server hostname: error # (error-message)
```

Hinweis – Wegen der möglichen Fehler sollten Sie keine Dateisysteme weich einhängen, in denen Daten mit Lese- und Schreibzugriff oder Dateisysteme enthalten sind, in denen ausführbare Dateien ausgeführt werden. Wenn die Fehler von der Anwendung ignoriert werden, können beschreibbare Daten beschädigt werden. Eingehängte ausführbare Dateien können unter Umständen nicht richtig geladen werden und funktionieren dann nicht ordnungsgemäß.

NFS-Fehlerbehebungsverfahren

Um festzustellen, an welcher Stelle der NFS-Service fehlgeschlagen ist, müssen Sie verschiedene Verfahren durchführen, um den Ausfallpunkt zu isolieren. Prüfen Sie Folgendes:

- Kann der Client mit dem Server Kontakt aufnehmen?
- Kann der Client mit den NFS-Services auf dem Server Kontakt aufnehmen?
- Werden die NFS-Services auf dem Server ausgeführt?

Während der Prüfung werden Sie eventuell feststellen, dass andere Teile des Netzwerks nicht funktionieren, beispielsweise der Name Service oder die physische Netzwerkhardware.

Fehlersuchverfahren für verschiedene Name Services finden Sie im *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*. Während der Durchführung des Verfahrens werden Sie eventuell feststellen, dass die Clientseite nicht von dem Problem betroffen ist. Dies ist beispielsweise dann der Fall, wenn Sie mindestens eine Fehlermeldung aus jedem Teilnetz Ihres Arbeitsbereichs erhalten. Unter diesen Gegebenheiten ist davon auszugehen, dass der Server oder die Netzwerkhardware des Servers das Problem ist. Dann sollten Sie den Fehler beim Server und nicht beim Client suchen.

▼ So prüfen Sie die Konnektivität auf einem NFS-Client

1 **Prüfen Sie, ob der NFS-Server vom Client aus erreicht werden kann. Geben Sie auf dem Client den folgenden Befehl ein:**

```
% /usr/sbin/ping bee
bee is alive
```

Wenn gemeldet wird, dass der Server intakt ist, prüfen Sie den NFS-Server per Remote-Zugriff. Lesen Sie dazu „So prüfen Sie den NFS-Server per Remote-Zugriff“ auf Seite 127.

2 **Wenn der Server nicht vom Client erreicht werden kann, stellen Sie sicher, dass der lokale Name Service ausgeführt wird.**

Für NIS+-Clients geben Sie Folgendes ein:

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-58.acme.com.
        Last Update seen was Mon Jun  5 11:16:10 1995
```

3 **Wenn der Name Service ausgeführt wird, stellen Sie sicher, dass der Client die richtigen Hostinformationen erhalten hat, indem Sie Folgendes eingeben:**

```
% /usr/bin/getent hosts bee
129.144.83.117    bee.eng.acme.com
```

4 **Wenn die Hostinformationen korrekt sind, aber der Server nicht vom Client aus erreichbar ist, führen Sie den Befehl `ping` über einen anderen Client aus.**

Wenn der über den zweiten Client ausgeführte Befehl fehlschlägt, informieren Sie sich unter „So prüfen Sie den NFS-Service auf dem Server“ auf Seite 128.

5 **Wenn der Server über den zweiten Client erreicht werden kann, verwenden Sie `ping`, um die Konnektivität des ersten Clients mit anderen Systemen im lokalen Netzwerk zu prüfen.**

Wenn dieser Befehl fehlschlägt, prüfen Sie die Konfiguration der Netzwerksoftware auf dem Client, beispielsweise `/etc/netmasks` und `/etc/nsswitch.conf`.

6 **(Optional) Prüfen Sie die Ausgabe des Befehls `rpcinfo`.**

Wenn nach Ausführung des Befehls `rpcinfo` nicht die Meldung `program 100003 version 4 ready and waiting` angezeigt wird, ist die NFS-Version 4 nicht auf dem Server aktiviert. Informationen zur Aktivierung von NFS-Version 4 finden Sie in Tabelle 5–3.

7 **Wenn die Software in Ordnung ist, prüfen Sie die Netzwerkhardware.**

Versuchen Sie, den Client auf einen zweiten Netzwerkanschluss zu verschieben.

▼ So prüfen Sie den NFS-Server per Remote-Zugriff

Beachten Sie, dass die Unterstützung für die Protokolle UDP und MOUNT nicht nötig ist, wenn Sie einen Server der NFS-Version 4 verwenden.

1 **Stellen Sie sicher, dass die NFS-Services auf dem NFS-Server gestartet wurden, indem Sie den folgenden Befehl eingeben:**

```
% rpcinfo -s bee|egrep 'nfs|mountd'
 100003  3,2    tcp,udp,tcp6,upd6               nfs     superuser
 100005  3,2,1  ticots,ticotsord,tcp,tcp6,ticlts,udp,upd6  mountd  superuser
```

Wenn die Dämonen noch nicht gestartet wurden, informieren Sie sich unter „So starten Sie die NFS-Services neu“ auf Seite 130.

2 **Prüfen Sie, ob die `nfsd`-Prozesse des Servers antworten.**

Geben Sie auf dem Client den folgenden Befehl ein, um die UDP-NFS-Verbindungen vom Server zu prüfen.

```
% /usr/bin/rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

Hinweis – NFS-Version 4 bietet keine Unterstützung für UDP.

Wenn der Server ausgeführt wird, wird eine Liste von Programm- und Versionsnummern ausgegeben. Die TCP-Verbindung wird mithilfe der Option `-t` geprüft. Wenn dieser Befehl fehlschlägt, fahren Sie mit „So prüfen Sie den NFS-Service auf dem Server“ auf Seite 128 fort.

3 **Prüfen Sie, ob der Servereintrag `mountd` antwortet, indem Sie den folgenden Befehl eingeben:**

```
% /usr/bin/rpcinfo -u bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
```

Wenn der Server ausgeführt wird, wird eine Liste von Programm- und Versionsnummern ausgegeben, die dem UDP-Protokoll zugeordnet sind. Die TCP-Verbindung wird mithilfe der Option `-t` geprüft. Fahren Sie beim Fehlschlagen mit den Schritten unter „So prüfen Sie den NFS-Service auf dem Server“ auf Seite 128 fort.

4 **Prüfen Sie, ob der autofs-Service verwendet wird:**

```
% cd /net/wasp
```

Wählen Sie einen `/net`- oder `/home`-Einhängepunkt, von dem Sie wissen, dass er ordnungsgemäß funktioniert. Wenn dieser Befehl fehlschlägt, melden Sie sich als `root`-Benutzer beim Client an und geben Folgendes ein, um den autofs-Service neu zu starten:

```
# svcadm restart system/filesystem/autofs
```

5 **Stellen Sie sicher, dass das Dateisystem wie erwartet auf dem Server gemeinsam genutzt wird.**

```
% /usr/sbin/showmount -e bee
/usr/src                                    eng
/export/share/man                       (everyone)
```

Prüfen Sie den Eintrag auf dem Server und den Eintrag des lokalen Einhängepunkts auf Fehler. Prüfen Sie auch den Namespace. Wenn sich der erste Client in dieser Situation nicht in der `eng`-Netzgruppe befindet, kann der Client nicht das `/usr/src` -Dateisystem einhängen.

Prüfen Sie in den lokalen Dateien alle Einträge, die Einhängeinformationen enthalten. Die Liste schließt `/etc/vfstab` und alle `/etc/auto_*` -Dateien ein.

▼ So prüfen Sie den NFS-Service auf dem Server

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Prüfen Sie, ob der Server die Clients erreichen kann.**

```
# ping lilac
lilac is alive
```

3 **Wenn der Client nicht vom Server erreicht werden kann, stellen Sie sicher, dass der lokale Name Service ausgeführt wird.**

Für NIS+-Clients geben Sie Folgendes ein:

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-58.acme.com.
        Last Update seen was Mon Jun  5 11:16:10 1995
```

4 **Wenn der Name Service ausgeführt wird, prüfen Sie die Konfiguration der Netzwerksoftware auf dem Server, beispielsweise `/etc/netmasks` und `/etc/nsswitch.conf`.**

5 **Geben Sie den folgenden Befehl ein, um zu prüfen, ob der `rpcbind`-Dämon ausgeführt wird.**

```
# /usr/bin/rpcinfo -u localhost rpcbind
program 100000 version 1 ready and waiting
program 100000 version 2 ready and waiting
program 100000 version 3 ready and waiting
```

Wenn der Server ausgeführt wird, wird eine Liste von Programm- und Versionsnummern ausgegeben, die dem UDP-Protokoll zugeordnet sind. Wenn `rpcbind` offensichtlich hängt, starten Sie den Server neu.

6 **Geben Sie den folgenden Befehl ein, um zu prüfen, ob der `nfsd`-Dämon ausgeführt wird.**

```
# rpcinfo -u localhost nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
# ps -ef | grep nfsd
root    232      1  0  Apr 07     ?     0:01 /usr/lib/nfs/nfsd -a 16
root   3127   2462  1  09:32:57  pts/3  0:00 grep nfsd
```

Hinweis – NFS-Version 4 bietet keine Unterstützung für UDP.

Wenn der Server ausgeführt wird, wird eine Liste von Programm- und Versionsnummern ausgegeben, die dem UDP-Protokoll zugeordnet sind. Sie können auch die Option `-t` mit `rpcinfo` verwenden, um die TCP-Verbindung zu prüfen. Wenn diese Befehle fehlschlagen, starten Sie den NFS-Service neu. Lesen Sie dazu „So starten Sie die NFS-Services neu“ auf Seite 130.

7 **Geben Sie den folgenden Befehl ein, um zu prüfen, ob der `mountd`-Dämon ausgeführt wird.**

```
# /usr/bin/rpcinfo -u localhost mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
# ps -ef | grep mountd
root    145      1 0 Apr 07  ?     21:57 /usr/lib/autofs/automountd
root    234      1 0 Apr 07  ?     0:04  /usr/lib/nfs/mountd
root   3084 2462 1 09:30:20 pts/3  0:00  grep mountd
```

Wenn der Server ausgeführt wird, wird eine Liste von Programm- und Versionsnummern ausgegeben, die dem UDP-Protokoll zugeordnet sind. Sie können auch die Option `-t` mit `rpcinfo` verwenden, um die TCP-Verbindung zu prüfen. Wenn diese Befehle fehlschlagen, starten Sie den NFS-Service neu. Lesen Sie dazu „So starten Sie die NFS-Services neu“ auf Seite 130.

▼ So starten Sie die NFS-Services neu

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Starten Sie den NFS-Service auf dem Server.**

Geben Sie folgenden Befehl ein:

```
# svcadm restart network/nfs/server
```

Feststellen, welcher Host den NFS-Dateiservice bereitstellt

Führen Sie den Befehl `nfsstat` mit der Option `-m` aus, um aktuelle NFS-Informationen zu sammeln. Der Name des aktuellen Servers steht hinter `currserver=`.

```
% nfsstat -m
/usr/local from bee,wasp:/export/share/local
 Flags: vers=3,proto=tcp,sec=sys,hard,intr,llock,link,synlink,
        acl,rsize=32768,wsize=32678,retrans=5
 Failover: noresponse=0, failover=0, remap=0, currserver=bee
```

▼ So prüfen Sie Optionen, die in Verbindung mit dem Befehl `mount` verwendet werden

Es wird keine Warnung für ungültige Optionen ausgegeben. Anhand des folgenden Verfahrens kann festgestellt werden, ob die über die Befehlszeile oder `/etc/vfstab` angegebenen Optionen gültig sind.

In diesem Beispiel wurde der folgende Befehl ausgeführt:

```
# mount -F nfs -o ro,vers=2 bee:/export/share/local /mnt
```

1 **Prüfen Sie die Optionen, indem Sie den folgenden Befehl ausführen:**

```
% nfsstat -m
/mnt from bee:/export/share/local
Flags:  vers=2,proto=tcp,sec=sys,hard,intr,dynamic,acl,rsize=8192,wsize=8192,
        retrans=5
```

Das Dateisystem von bee wurde eingehängt, wobei die Protokollversion auf 2 gesetzt war. Leider werden mithilfe des Befehls `nfsstat` nicht alle Informationen zu den Optionen angezeigt. Die Verwendung des Befehls `nfsstat` ist jedoch die beste Methode, um die Optionen zu prüfen.

2 **Prüfen Sie den Eintrag in `/etc/mnttab`.**

Der Befehl `mount` lässt nicht zu, dass ungültige Optionen in die Einhängetabelle eingefügt werden. Prüfen Sie darum, ob die in der Datei aufgeführten Optionen mit den Optionen übereinstimmen, die in der Befehlszeile aufgeführt sind. Auf diese Weise können Sie die Optionen überprüfen, die nicht durch den Befehl `nfsstat` gemeldet wurden.

```
# grep bee /etc/mnttab
bee:/export/share/local /mnt nfs    ro,vers=2,dev=2b0005e 859934818
```

autofs-Fehlerbehebung

Gelegentlich können Probleme mit autofs auftreten. Dieser Abschnitt dient zur Verbesserung des Problemlösungsprozesses. Der Abschnitt ist in zwei Unterabschnitte gegliedert.

In diesem Abschnitt werden Fehlermeldungen aufgelistet, die von autofs generiert werden. Die Liste besteht aus zwei Teilen:

- Fehlermeldungen, die von der ausführlichen Option (`-v`) von `automount` generiert werden
- Fehlermeldungen, die jederzeit angezeigt werden können

Nach jeder Fehlermeldung folgt eine Beschreibung und die wahrscheinliche Ursache der Meldung.

Zur Durchführung einer Fehlerbehebung starten Sie die autofs-Programme mit der ausführlichen Option (`-v`). Anderenfalls können Sie mit Problemen konfrontiert werden, ohne die Ursache zu kennen.

In den folgenden Abschnitten werden die Fehlermeldungen sowie Beschreibungen der möglichen Probleme aufgeführt, die angezeigt werden, wenn autofs fehlschlägt.

Von `automount -v` generierte Fehlermeldungen

`bad key` *key* `in direct map`*mapname*

Beschreibung: Beim Abfragen einer direkten Map hat autofs einen Eintragsschlüssel ohne Schrägstrich (/) als Präfix gefunden.

Lösung: Schlüssel in direkten Maps müssen volle Pfadnamen sein.

`bad key` *key* `in indirect map` *mapname*

Beschreibung: Beim Abfragen einer indirekten Map hat autofs einen Eintragsschlüssel gefunden, der einen Schrägstrich (`/`) enthält.

Lösung: Die Schlüssel von indirekten Maps müssen mit einfachen Namen beginnen, nicht mit Pfadnamen.

`can't mount` *server*`:`*pathname: reason*
Beschreibung: Der Einhängedämon auf dem Server verweigert die Bereitstellung einer Dateizugriffsroutine *server*:*pathname* .

Lösung: Prüfen Sie die Exporttabelle auf dem Server.

`couldn't create mount point` *mountpoint*`:` *reason*
Beschreibung: Autofs konnte keinen für den Einhängevorgang benötigten Einhängepunkt erstellen. Dieses Problem tritt häufig auf, wenn Sie versuchen, alle exportierten Dateisysteme eines Servers hierarchisch einzuhängen.

Lösung: Ein benötigter Einhängepunkt kann nur in einem Dateisystem vorhanden sein, das nicht eingehängt werden kann, was bedeutet, dass das Dateisystem nicht exportiert werden kann. Der Einhängepunkt kann nicht erstellt werden, weil das exportierte übergeordnete Dateisystem in schreibgeschütztem Zustand exportiert wird.

`leading space in map entry` *entry* `text in` *mapname*
Beschreibung: Autofs hat in einer automount-Map einen Eintrag entdeckt, der führende Leerzeichen enthält. Dieses Problem deutet in der Regel auf einen nicht richtig fortgeführten Map-Eintrag hin. Beispiel:

```
fake
/blat           frobz:/usr/frotz
```

Lösung: In diesem Beispiel wird eine Warnung ausgegeben, wenn autofs die zweite Zeile vorfindet, weil die erste Zeile nicht durch einen umgekehrten Schrägstrich (\) abgeschlossen ist.

mapname `: Not found`
Beschreibung: Die erforderliche Map kann nicht gefunden werden. Diese Meldung wird nur dann ausgegeben, wenn die Option `-v` verwendet wird.

Lösung: Prüfen Sie die Schreibweise und den Pfadnamen des Namens der Map.

`remount` *server*`:`*pathname* `on` *mountpoint* `: server not responding`
Beschreibung: Autofs konnte das zuvor ausgehängte Dateisystem nicht wieder einhängen.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese äußerst seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`WARNING:` *mountpoint* `already mounted on`
Beschreibung: Autofs versucht, eine Einhängung über einen vorhandenen Einhängepunkt auszuführen. Diese Meldung zeigt an, dass ein interner Fehler in autofs aufgetreten ist.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese äußerst seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

Verschiedene Fehlermeldungen

`dir` *mountpoint* `must start with '/'`
Lösung: Der Automounter-Einhängepunkt muss als vollständiger Pfadname angegeben sein. Prüfen Sie die Schreibweise und den Pfadnamen des Einhängepunkts.

`hierarchical mountpoint:` *pathname1* `and` *pathname2*
Lösung: Autofs lässt keine hierarchische Beziehung zwischen seinen Einhängepunkten zu. Ein autofs-Einhängepunkt darf nicht in einem anderen automatisch eingehängten Dateisystem enthalten sein.

`host` *server* `not responding`
Beschreibung: Autofs hat vergeblich versucht, mit *server* Kontakt aufzunehmen.

Lösung: Prüfen Sie den Status des NFS-Servers.

hostname`: exports:` *rpc-err*
Beschreibung: Beim Abrufen der Exportliste von *hostname* ist ein Fehler aufgetreten. Diese Meldung deutet auf ein Server- oder Netzwerkproblem hin.

Lösung: Prüfen Sie den Status des NFS-Servers.

`map` *mapname*`, key` *key*`: bad`
Beschreibung: Der Map-Eintrag ist unlesbar und kann nicht von autofs interpretiert werden.

Lösung: Prüfen Sie den Eintrag erneut. Eventuell sind im Eintrag Zeichen enthalten, die unterbrochen werden müssen.

mapname`:` *nis-err*
Beschreibung: Während der Suche nach einem Eintrag in einer NIS-Map ist ein Fehler aufgetreten. Diese Meldung kann auf NIS-Probleme hindeuten.

Lösung: Prüfen Sie den Status des NIS-Servers.

`mount of` *server*`:`*pathname* `on` *mountpoint*`:`*reason*
Beschreibung: Autofs konnte keine Einhängung durchführen. Dies kann auf ein Server- oder Netzwerkproblem hindeuten. In der *reason*-Zeichenfolge wird das Problem definiert.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese äußerst seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

mountpoint`: Not a directory`
Beschreibung: Autofs ist kein Verzeichnis und kann sich nicht selbst an *mountpoint* einhängen.

Lösung: Prüfen Sie die Schreibweise und den Pfadnamen des Einhängepunkts.

`nfscast: cannot send packet:` *reason*
Beschreibung: Autofs kann kein Abfragepaket an einen Server senden, der in einer Liste der Speicherorte von replizierten Dateisystemen aufgeführt ist. In der *reason*-Zeichenfolge wird das Problem definiert.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese äußerst seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`nfscast: cannot receive reply:` *reason*
Beschreibung: Autofs kann keine Antwort von einem der Server empfangen, die in einer Liste der Speicherorte von replizierten Dateisystemen aufgeführt sind. In der *reason*-Zeichenfolge wird das Problem definiert.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese äußerst seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`nfscast: select:` *reason*
Beschreibung: Fehlermeldungen dieser Art deuten auf Probleme hin, die aus dem Versuch resultieren, Server auf ein repliziertes Dateisystem zu prüfen. Diese Meldung kann auf ein Netzwerkproblem hindeuten. In der *reason*-Zeichenfolge wird das Problem definiert.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese äußerst seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`pathconf: no info for` *server*`:`*pathname*
Beschreibung: Autofs konnte keine `pathconf`-Informationen für den Pfadnamen abrufen.

Lösung: Weitere Informationen finden Sie auf der Manpage `fpathconf(2)`.

`pathconf:` *server* `: server not responding`
Beschreibung: Autofs kann keinen Kontakt mit dem Einhängedämon auf dem Server aufnehmen, der die Informationen für `pathconf()` bereitstellt.

Lösung: Vermeiden Sie es, in Verbindung mit diesem Server die Einhängeoption `POSIX` zu verwenden.

Weitere Fehler mit Autofs

Wenn in den `/etc/auto*`-Dateien das Ausführungsbit gesetzt ist, versucht der Automounter, die Map auszuführen, wodurch Meldungen wie die folgende ausgegeben werden:

```
/etc/auto_home: +auto_home: not found
```

In solche einem Fall weist die `auto_home`-Datei ungültige Berechtigungen auf. Durch jeden Eintrag in der Datei wird eine Fehlermeldung ausgegeben, die der obigen Meldung ähnlich ist. Sie können die Berechtigungen der Datei zurücksetzen, indem Sie den folgenden Befehl eingeben:

```
# chmod 644 /etc/auto_home
```

NFS-Fehlermeldungen

In diesem Abschnitt werden Fehlermeldungen, eine Beschreibung der Bedingungen, die zum jeweiligen Fehler führen, sowie mindestens eine Abhilfemaßnahme aufgeführt.

`Bad argument specified with index option - must be a file`
Lösung: Sie müssen zusammen mit der Option `index` einen Dateinamen angeben. Sie können keine Verzeichnisnamen verwenden.

`Cannot establish NFS service over /dev/`*tcp*`: transport setup problem`
Beschreibung: Diese Meldung wird häufig ausgegeben, wenn die Informationen zu den Services im Namespace nicht aktualisiert wurden. Die Meldung kann auch für UDP ausgegeben werden.

Lösung: Um dieses Problem zu beheben, müssen Sie die Daten der Services im Namespace aktualisieren.

Die Einträge für NIS+ sollten wie folgt aussehen:

```
nfsd nfsd tcp 2049 NFS server daemon
nfsd nfsd udp 2049 NFS server daemon
```

Die Einträge für NIS und `/etc/services` sollten wie folgt aussehen:

```
nfsd    2049/tcp    nfs    # NFS server daemon
nfsd    2049/udp    nfs    # NFS server daemon
```

`Cannot use index option without public option`
Lösung: Fügen Sie die Option `public` mit der Option `index` in den share-Befehl ein. Sie müssen die Routine für den Zugriff auf öffentliche Dateien definieren, damit die Option `index` funktioniert.

Hinweis – Bei Verwendung von Solaris 2.5.1 musste die Routine für den Zugriff auf öffentliche Dateien mithilfe des Befehls `share` definiert werden. In Solaris 2.6 ist die Routine für den Zugriff auf öffentliche Dateien standardmäßig auf `root` (`/`) gesetzt. Diese Fehlermeldung ist nicht mehr relevant.

`Could not start` *daemon*`:` *error*
Beschreibung: Diese Fehlermeldung wird angezeigt, wenn der Dämon nicht ordnungsgemäß beendet wird oder ein Systemaufruffehler auftritt. In der *error*-Zeichenfolge wird das Problem definiert.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`Could not use public filehandle in request to` *server*
Beschreibung: Diese Meldung wird angezeigt, wenn die Option `public` angegeben ist, aber der NFS-Server nicht die Routine für den Zugriff auf öffentliche Dateien unterstützt. In solch einem Fall schlägt das Einhängen fehl.

Lösung: Um dieses Problem zu beheben, versuchen Sie entweder, die Einhängungsanforderung ohne die Routine für den Zugriff auf öffentliche Dateien weiterzugeben, oder den NFS-Server neu zu konfigurieren, um die Routine für den Zugriff auf öffentliche Dateien zu unterstützen.

daemon `running already with pid` *pid*
Beschreibung: Der Dämon wird bereits ausgeführt.

Lösung: Um eine neue Instanz auszuführen, brechen Sie die aktuelle Version ab und starten eine neue Version.

`error locking` *lock file*
Beschreibung: Diese Meldung wird angezeigt, wenn die Sperrdatei (*lock file*), die einem Dämon zugeordnet ist, nicht richtig gesperrt werden kann.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`error checking` *lock file*`:` *error*
Beschreibung: Diese Meldung wird angezeigt, wenn die Sperrdatei (*lock file*), die einem Dämon zugeordnet ist, nicht richtig geöffnet werden kann.

Lösung: Wenden Sie sich an Oracle, um Hilfe anzufordern. Für diese seltene Fehlermeldung ist kein direkter Lösungsansatz vorhanden.

`NOTICE: NFS3: failing over from` *host1* `to` *host2*
Beschreibung: Diese Meldung wird an der Konsole angezeigt, wenn ein Failover stattfindet. Die Meldung dient nur zur Information.

Lösung: Es ist keine Maßnahme erforderlich.

filename`: File too large`
Beschreibung: Ein Client der NFS-Version 2 versucht, auf eine Datei zuzugreifen, die größer als 2 GB ist.

Lösung: Die Verwendung der NFS-Version 2 ist zu vermeiden. Hängen Sie das Dateisystem mit Version 3 oder 4 ein. Eine Beschreibung der Option `nolargefiles` finden Sie unter „`mount`-Optionen für NFS-Dateisysteme“ auf Seite 163.

`mount: ... server not responding:RPC_PMAP_FAILURE - RPC_TIMED_OUT`
Beschreibung: Der Server, der das Dateisystem nutzt, das Sie gerade einzuhängen versuchen, ist ausgefallen, nicht erreichbar, wird auf der falschen Betriebsebene ausgeführt, oder sein Dämon `rpcbind` ist ausgefallen oder hängt.

Lösung: Warten Sie auf den Neustart des Servers. Wenn der Server hängt, starten Sie den Server neu.

`mount: ... server not responding: RPC_PROG_NOT_REGISTERED`
Beschreibung: Die Einhängungsanforderung wurde bei `rpcbind` registriert, aber der NFS-Einhängungsdämon `mountd` ist nicht registriert.

Lösung: Warten Sie auf den Neustart des Servers. Wenn der Server hängt, starten Sie den Server neu.

`mount: ... No such file or directory`
Beschreibung: Entweder das Remote-Verzeichnis oder das lokale Verzeichnis ist nicht vorhanden.

Lösung: Prüfen Sie die Schreibweise der Verzeichnisnamen. Führen Sie `ls` für beide Verzeichnisse aus.

`mount: ...: Permission denied`
Beschreibung: Eventuell ist der Name Ihres Computers nicht in der Liste der Clients oder der Netzgruppe enthalten, die die Berechtigung hat, auf das Dateisystem zuzugreifen, das Sie einzuhängen versuchen.

Lösung: Verwenden Sie `showmount -e`, um die Zugriffsliste zu prüfen.

`NFS file temporarily unavailable on the server, retrying ...`
Beschreibung: Ein Server der NFS-Version 4 kann die Verwaltung einer Datei an einen Client delegieren. Diese Meldung zeigt an, dass der Server erneut eine Delegierung für einen anderen Client aufruft, die mit einer Anforderung von Ihrem Client in Konflikt steht.

Lösung: Der erneute Aufruf muss stattfinden, bevor der Server die Anforderung des Clients verarbeiten kann. Weitere Informationen zur Delegierung finden Sie unter „Delegierung in NFS-Version 4“ auf Seite 195.

`NFS fsstat failed for server` *hostname*`: RPC: Authentication error`
Beschreibung: Dieser Fehler kann auf viele Ursachen zurückzuführen sein. Die Behebung dieses Problems ist äußerst schwierig, wenn das Problem darauf zurückzuführen ist, dass

ein Benutzer in zu vielen Gruppen aktiv ist. Derzeit kann ein Benutzer in maximal 16 Gruppen aktiv sein, wenn er über NFS-Einhängepunkte auf Dateien zugreift.

Lösung: Eine alternative Möglichkeit gibt es für Benutzer, die in mehr als 16 Gruppen aktiv sein müssen. Sie können auf Zugriffskontrolllisten zugreifen, um die erforderlichen Zugriffsberechtigungen bereitzustellen.

`nfs mount: ignoring invalid option "-`*option*`"`
Beschreibung: Das Flag *-option* ist ungültig.

Lösung: Informationen zum Prüfen der erforderlichen Syntax finden Sie auf der Manpage `mount_nfs(1M)`.

Hinweis – Diese Fehlermeldung wird nicht angezeigt, wenn eine Version des Befehls `mount` ausgeführt wird, der in Solaris ab Version 2.6 bis zur neuesten Version oder in früheren gepatchten Versionen enthalten ist.

`nfs mount: NFS can't support "nolargefiles"`
Beschreibung: Ein NFS-Client hat versucht, ein Dateisystem von einem NFS-Server mithilfe der Option `-nolargefiles` einzuhängen.

Lösung: Diese Option wird nicht für NFS-Dateisysteme unterstützt.

`nfs mount: NFS V2 can't support "largefiles"`
Beschreibung: Das Protokoll der NFS-Version 2 kann keine großen Dateien verarbeiten.

Lösung: Sie müssen die Version 3 oder 4 verwenden, wenn auf große Dateien zugegriffen werden muss.

`NFS server` *hostname* `not responding still trying`
Beschreibung: Wenn Programme hängen, während dateibezogenen Vorgänge ausgeführt werden, ist Ihr NFS-Server möglicherweise ausgefallen. Diese Meldung zeigt an, dass der NFS-Server *hostname* ausgefallen ist oder ein Server- oder Netzwerkproblem vorliegt.

Lösung: Wenn Failover verwendet wird, ist *hostname* eine Liste von Servern. Beginnen Sie mit der Fehlerbehebung anhand des Verfahrens, das unter „So prüfen Sie die Konnektivität auf einem NFS-Client“ auf Seite 126 beschrieben ist.

`NFS server recovering`
Beschreibung: Während des Neustarts des Servers der NFS-Version 4 wurden einige Vorgänge nicht zugelassen. Diese Meldung zeigt an, dass der Client auf die Genehmigung des Servers wartet, damit der Vorgang fortgesetzt werden kann.

Lösung: Es ist keine Maßnahme erforderlich. Warten Sie, bis der Server den Vorgang zulässt.

`Permission denied`

Beschreibung: Diese Meldungen, die durch die Befehle `ls -l`, `getfacl` und `setfacl` angezeigt werden, sind auf die folgenden Ursachen zurückzuführen:

- Wenn ein Benutzer, der in einem Zugriffskontrolllisteneintrag auf einem Server der NFS-Version 4 angegeben ist, oder eine Gruppe, die in einem solchen Eintrag angegeben ist, nicht einem gültigen Benutzer oder einer gültigen Gruppe auf einem Client der NFS-Version 4 zugeordnet werden kann, wird dem Benutzer bzw. der Gruppe nicht gestattet, die Zugriffskontrollliste auf dem Client zu lesen.
- Wenn der Benutzer, der in einem Zugriffskontrolllisteneintrag angegeben ist, der auf einem Client der NFS-Version 4 definiert wird, oder die Gruppe, die in einem solchen Eintrag angegeben ist, nicht einem gültigen Benutzer oder einer gültigen Gruppe auf einem Server der NFS-Version 4 zugeordnet werden kann, wird dem Benutzer bzw. der Gruppe nicht gestattet, die Zugriffskontrollliste auf dem Client zu beschreiben oder zu modifizieren.
- Wenn ein Client und ein Server der NFS-Version 4 nicht übereinstimmende NFSMAPID_DOMAIN-Werte aufweisen, kann die ID nicht zugeordnet werden.

Weitere Informationen finden Sie unter „Zugriffskontrolllisten (ACLs) und `nfsmapid` in NFS-Version 4“ auf Seite 197.

Lösung: Führen Sie folgende Schritte aus:

- Stellen Sie sicher, dass alle Benutzer- und Gruppen-IDs in den Einträgen der Zugriffssteuerungsliste sowohl auf dem Client als auch auf dem Server vorhanden sind.
- Stellen Sie sicher, dass der Wert für NFSMAPID_DOMAIN in der `/etc/default/nfs`-Datei korrekt angegeben ist. Weitere Informationen finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144.

Um festzustellen, ob ein Benutzer oder eine Gruppe nicht auf dem Server oder Client zugeordnet werden kann, verwenden Sie das unter „Prüfen auf nicht zugeordnete Benutzer- oder Gruppen-IDs“ auf Seite 199 genannte Skript.

`port` *number* `in nfs URL not the same as port` *number* `in port option`

Beschreibung: Die in der NFS-URL enthaltene Portnummer muss mit der Portnummer übereinstimmen, die in der Option `-port` für das Einhängen enthalten ist. Wenn die Portnummern nicht übereinstimmen, schlägt das Einhängen fehl.

Lösung: Entweder verwenden Sie einen anderen Befehl, um für die Übereinstimmung der Portnummern zu sorgen, oder geben Sie keine Portnummer an, die falsch ist. Normalerweise ist es nicht nötig, die Portnummer sowohl für die NFS-URL als auch für die Option `-port` anzugeben.

`replicas must have the same version`

Beschreibung: Damit das NFS-Failover richtig funktioniert, müssen die NFS-Server, die Replikationen sind, dieselbe Version des NFS-Protokolls unterstützen.

Lösung: Das Ausführen mehrerer Versionen ist nicht zulässig.

`replicated mounts must be read-only`
Beschreibung: Das NFS-Failover funktioniert nicht bei Dateisystemen, die mit Lese- und Schreibzugriff eingehängt werden. Wenn ein Dateisystem mit Lese- und Schreibzugriff eingehängt wird, steigt die Wahrscheinlichkeit, dass eine Datei geändert wird.

Lösung: Für das NFS-Failover müssen Dateisysteme identisch sein.

`replicated mounts must not be soft`
Beschreibung: Replizierte Einhängungen erfordern, dass Sie auf eine Zeitüberschreitung warten. Erst dann findet ein Failover statt.

Lösung: Die Option `soft` erfordert, dass die Einhängung sofort fehlschlägt, wenn eine Zeitüberschreitung beginnt. Aus diesem Grund können Sie die Option `-soft` nicht für einen replizierten Einhängung verwenden.

`share_nfs: Cannot share more than one filesystem with 'public' option`
Lösung: Stellen Sie sicher, dass durch die `/etc/dfs/dfstab`-Datei nur ein einziges Dateisystem angegeben ist, das mithilfe der Option `-public` gemeinsam genutzt wird. Pro Server kann nur eine Routine für den Zugriff auf öffentliche Dateien definiert werden. Aus diesem Grund kann nur ein Dateisystem pro Server mit dieser Option gemeinsam genutzt werden.

`WARNING: No network locking on` *hostname*`:` *path*`: contact admin to install server change`
Beschreibung: Ein NFS-Client hat vergeblich versucht, eine Verbindung mit dem Netzwerk-Sperren-Manager auf einem NFS-Server herzustellen. Diese Warnung wird aufgrund der nicht funktionierenden Sperrung ausgegeben, nicht aber aufgrund der fehlgeschlagenen Einhängung.

Lösung: Aktualisieren Sie den Server mit einer neuen Version des Betriebssystems, das vollständige Unterstützung des Sperren-Managers bietet.

◆ ◆ ◆ KAPITEL 6

Zugreifen auf Netzwerkdateisysteme (Referenz)

In diesem Kapitel werden NFS-Befehle erläutert, sowie verschiedene Teile der NFS-Umgebung und deren Zusammenwirken.

- „NFS-Dateien“ auf Seite 141
- „NFS-Dämonen“ auf Seite 147
- „NFS-Befehle“ auf Seite 160
- „Befehle zum Beheben von NFS-Problemen“ auf Seite 179
- „NFS über RDMA“ auf Seite 185
- „Funktionsweise des NFS-Service“ auf Seite 186
- „Autofs-Maps“ auf Seite 212
- „Funktionsweise von autofs“ auf Seite 219
- „Autofs-Referenz“ auf Seite 232

Hinweis – Wenn auf Ihrem System aktivierte Zonen vorhanden sind und Sie beabsichtigen, diese Funktion in einer nicht globalen Zone zu verwenden, lesen Sie *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*, um weitere Informationen zu erhalten.

NFS-Dateien

Sie benötigen verschiedene Dateien, um auf Computern ausgeführte NFS-Vorgänge zu unterstützen. Viele dieser Dateien sind ASCII-Dateien, aber einige sind Datendateien. In Tabelle 6–1 sind diese Dateien und ihre Funktionen aufgeführt.

TABELLE 6–1 NFS-Dateien

Dateiname	Funktion
`/etc/default/autofs`	Listet Konfigurationsinformationen zur autofs-Umgebung auf.
`/etc/default/fs`	Listet das standardmäßige Dateisystem der lokalen Dateisysteme auf.

TABELLE 6–1 NFS-Dateien *(Fortsetzung)*

Dateiname	Funktion
`/etc/default/nfs`	Listet Konfigurationsinformationen zu `lockd` und `nfsd` auf. Weitere Informationen finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144 und auf der Manpage `nfs(4)`.
`/etc/default/nfslogd`	Listet Konfigurationsinformationen zum Protokollierungsdämon `nfslogd` des NFS-Servers auf.
`/etc/dfs/dfstab`	Listet die lokalen Ressourcen auf, die gemeinsam genutzt werden sollen.
`/etc/dfs/fstypes`	Listet die standardmäßigen Dateisysteme der Remote-Dateisysteme auf.
`/etc/dfs/sharetab`	Listet die lokalen und Remote-Ressourcen auf, die gemeinsam genutzt werden sollen. Weitere Informationen finden Sie auf der Manpage `sharetab(4)`. Bearbeiten Sie diese Datei nicht.
`/etc/mnttab`	Listet Dateisysteme auf, die derzeit eingehängt sind (einschließlich automatisch eingehängte Verzeichnisse). Weitere Informationen finden Sie auf der Manpage `mnttab(4)`. Bearbeiten Sie diese Datei nicht.
`/etc/netconfig`	Listet die Transportprotokolle auf. Bearbeiten Sie diese Datei nicht.
`/etc/nfs/nfslog.conf`	Listet allgemeine Konfigurationsinformationen zur Protokollierung des NFS-Servers auf.
`/etc/nfs/nfslogtab`	Listet Informationen zur Protokollnachverarbeitung durch `nfslogd` auf. Bearbeiten Sie diese Datei nicht.
`/etc/nfssec.conf`	Listet NFS-Sicherheitsservices auf.
`/etc/rmtab`	Listet Dateisysteme auf, die per Remote-Zugriff von NFS-Clients eingehängt wurden. Weitere Informationen finden Sie auf der Manpage `rmtab(4)`. Bearbeiten Sie diese Datei nicht.
`/etc/vfstab`	Definiert Dateisysteme, die lokal eingehängt werden sollen. Weitere Informationen finden Sie auf der Manpage `vfstab(4)`.

Der erste Eintrag in `/etc/dfs/fstypes` wird oft als standardmäßiges Dateisystem für die Remote-Dateisysteme verwendet. Dieser Eintrag definiert das NFS-Dateisystem als standardmäßiges Dateisystem.

In `/etc/default/fs` ist nur ein Eintrag enthalten: das standardmäßige Dateisystem für lokale Festplatten. Sie können feststellen, welche Dateisysteme auf einem Client oder Server unterstützt werden, indem Sie die Dateien in `/kernel/fs` prüfen.

/etc/default/autofs-Datei

Ab Solaris 10 können Sie die `/etc/default/autofs`-Datei verwenden, um Ihre autofs-Umgebung zu konfigurieren. Mit dieser Datei steht jetzt eine weitere Möglichkeit zum Konfigurieren der autofs-Befehle und autofs-Dämonen zur Verfügung. Dieselben Angaben, die Sie normalerweise über die Befehlszeile eingeben, können jetzt in diese Konfigurationsdatei eingetragen werden. Im Gegensatz zur Eingabe über die Befehlszeile werden die Angaben in dieser Datei jedoch sogar beim Upgrade des Betriebssystems beibehalten. Außerdem müssen Sie kritische Startdateien nicht mehr aktualisieren, um das bestehende Verhalten der autofs-Umgebung beizubehalten. Sie können die erforderlichen Angaben machen, indem Sie für die Schlüsselwörter folgende Werte verwenden:

AUTOMOUNT_TIMEOUT
: Legt fest, wie lange ein Dateisystem inaktiv bleiben darf, bevor es ausgehängt wird. Dieses Schlüsselwort entspricht dem Argument `-t` für den Befehl `automount`. Der Standardwert ist 600.

AUTOMOUNT_VERBOSE
: Gibt Meldungen aus, die sich auf autofs-Ein- und -Aushängevorgänge sowie weniger wichtige Ereignisse beziehen. Dieses Schlüsselwort entspricht dem Argument `-v` für `automount`. Der Standardwert ist FALSE.

AUTOMOUNTD_VERBOSE
: Sendet ein Statusmeldungsprotokoll an die Konsole und entspricht dem Argument `-v` für den `automountd`-Dämon. Der Standardwert ist FALSE.

AUTOMOUNTD_NOBROWSE
: Aktiviert oder deaktiviert die Suchfunktion für alle autofs-Einhängepunkte und entspricht dem Argument `-n` für `automountd`. Der Standardwert ist FALSE.

AUTOMOUNTD_TRACE
: Erweitert alle Remote-Prozeduraufrufe (RPCs) und zeigt die erweiterten RPCs in der Standardausgabe an. Dieses Schlüsselwort entspricht dem Argument `-T` für `automountd`. Der Standardwert ist 0. Die Werte können zwischen 0 und 5 liegen.

AUTOMOUNTD_ENV
: Ermöglicht es, den verschiedenen Umgebungen unterschiedliche Werte zuzuweisen. Dieses Schlüsselwort entspricht dem Argument `-D` für `automountd`. Das Schlüsselwort AUTOMOUNTD_ENV kann mehrmals verwendet werden. Für die Umgebungszuordnungen müssen Sie jedoch separate Zeilen verwenden.

Weitere Informationen finden Sie auf den Manpages `automount`(1M) und `automountd`(1M). Informationen zur Verfahrensweise finden Sie unter „Konfigurieren der autofs-Umgebung mithilfe der `/etc/default/autofs`-Datei“ auf Seite 109.

Schlüsselwörter für die /etc/default/nfs-Datei

In NFS-Version 4 können die folgenden Schlüsselwörter in der `/etc/default/nfs`-Datei definiert werden. Lassen Sie von der Telefongesellschaft oder vom Serviceprovider die Geräte installieren, die von den Clientsystemen verwendet werden.

NFS_SERVER_VERSMIN
: Legt die mindestens erforderliche Version des NFS-Protokolls fest, das registriert und vom Server bereitgestellt werden soll. Ab Solaris 10 ist der Standardwert 2. Weitere gültige Werte sind 3 oder 4. Lesen Sie dazu „Einrichten von NFS-Services“ auf Seite 96.

NFS_SERVER_VERSMAX
: Legt die mindestens erforderliche Version des NFS-Protokolls fest, das registriert und vom Server bereitgestellt werden soll. Ab Solaris 10 ist der Standardwert 4. Weitere gültige Werte sind 2 oder 3. Lesen Sie dazu „Einrichten von NFS-Services“ auf Seite 96.

NFS_CLIENT_VERSMIN
: Legt die mindestens erforderliche Version des NFS-Protokolls fest, das vom NFS-Client verwendet werden soll. Ab Solaris 10 ist der Standardwert 2. Weitere gültige Werte sind 3 oder 4. Lesen Sie dazu „Einrichten von NFS-Services“ auf Seite 96.

NFS_CLIENT_VERSMAX
: Legt die höchste Version des NFS-Protokolls fest, das vom NFS-Client verwendet werden soll. Ab Solaris 10 ist der Standardwert 4. Weitere gültige Werte sind 2 oder 3. Lesen Sie dazu „Einrichten von NFS-Services“ auf Seite 96.

NFS_SERVER_DELEGATION
: Legt fest, ob die Delegierungsfunktion der NFS-Version 4 für den Server aktiviert wird. Wenn diese Funktion aktiviert ist, versucht der Server, Delegierungen für den Client der NFS-Version 4 bereitzustellen. Die Serverdelegierung ist standardmäßig aktiviert. Informationen zur Deaktivierung der Serverdelegierung finden Sie unter „So wählen Sie andere NFS-Versionen auf einem Server aus“ auf Seite 99. Weitere Informationen finden Sie unter „Delegierung in NFS-Version 4“ auf Seite 195.

NFSMAPID_DOMAIN
: Legt eine allgemeine Domain für Clients und Server fest. Setzt die standardmäßige Verwendung des lokalen DNS-Domainnamens außer Kraft. Aufgabenbezogene Informationen finden Sie unter „Einrichten von NFS-Services“ auf Seite 96. Lesen Sie dazu auch „`nfsmapid`-Dämon“ auf Seite 151.

`/etc/default/nfslogd`-Datei

Mit dieser Datei werden einige der Parameter definiert, die für die NFS-Serverprotokollierung verwendet werden. Folgende Parameter können definiert werden:

CYCLE_FREQUENCY
: Legt die Anzahl von Stunden fest, die verstreichen müssen, bevor die Protokolldateien zyklisch durchlaufen werden. Der Standardwert beträgt 24 Stunden. Diese Option wird verwendet, um zu verhindern, dass die Protokolldateien zu groß werden.

IDLE_TIME
: Legt die Dauer der Inaktivität von `nfslogd` in Sekunden fest, bevor in der Pufferdatei nach weiteren Informationen gesucht wird. Durch diesen Parameter wird auch festgelegt, wie of die Konfigurationsdatei geprüft wird. Durch diesen Parameter und MIN_PROCESSING_SIZE wird festgelegt, wie oft die Pufferdatei verarbeitet wird. Der Standardwert beträgt 300 Sekunden. Durch eine Erhöhung dieses Werts kann die Leistung verbessert werden, da die Anzahl der Prüfungen verringert wird.

MAPPING_UPDATE_INTERVAL
: Gibt die Dauer in Sekunden zwischen den Aktualisierungen der Datensätze in den Dateizugriffsroutine-zu-Pfad-Maps an. Der Standardwert beträgt 86400 Sekunden oder ein (1) Tag. Dieser Parameter trägt dazu bei, dass die Dateizugriffsroutine-zu-Pfad-Maps immer auf dem neuesten Stand sind, ohne dass die Tabellen ständig aktualisiert werden müssen.

MAX_LOGS_PRESERVE
: Legt die Anzahl der Protokolldateien fest, die gespeichert werden sollen. Der Standardwert ist 10.

MIN_PROCESSING_SIZE
: Legt die Mindestanzahl der Bytes fest, die in der Pufferdatei erreicht werden muss, bevor eine Verarbeitung stattfindet und die Daten in die Protokolldatei geschrieben werden. Durch diesen Parameter und IDLE_TIME wird festgelegt, wie oft die Pufferdatei verarbeitet wird. Der Standardwert beträgt 524288 Byte. Durch eine Erhöhung dieses Werts kann die Leistung verbessert werden, da die Häufigkeit der Verarbeitung der Pufferdatei verringert wird.

PRUNE_TIMEOUT
: Legt die Anzahl von Stunden fest, die verstreichen müssen, bevor durch einen Zuordnungsdatensatz (zum Zuordnen einer Dateizugriffsroutine zu einem Pfad) eine Zeitüberschreitung ausgelöst wird und der Wert des Datensatzes reduziert werden kann. Der Standardwert beträgt 168 Stunden oder sieben Tage.

UMASK
: Gibt die Erstellungsmaske des Dateimodus für die Protokolldateien an, die von `nfslogd` erstellt werden. Der Standardwert ist 0137.

`/etc/nfs/nfslog.conf`-Datei

Diese Datei definiert den Pfad, Dateinamen und die Art der Protokollierung, die von `nfslogd` verwendet werden sollen. Jede Definition ist mit einem *tag* verbunden. Das Starten der

NFS-Serverprotokollierung erfordert, dass Sie das *tag* für jedes Dateisystem identifizieren. Das globale Tag dient zum Definieren der Standardwerte. Für jedes Tag können Sie nach Bedarf die folgenden Parameter definieren:

defaultdir=*path*
: Gibt den standardmäßigen Verzeichnispfad für die Protokollierungsdateien an. Wenn Sie keine andere Angabe machen, wird `/var/nfs` als Standardverzeichnis verwendet.

log=*path/filename*
: Legt den Pfad und den Dateinamen für die Protokolldateien fest. Die Standardeinstellung ist `/var/nfs/nfslog`.

fhtable=*path/filename*
: Legt den Pfad und den Dateinamen für die Dateizugriffsroutine-zu-Pfad-Datenbankdateien fest. Die Standardeinstellung ist `/var/nfs/fhtable`.

buffer=*path/filename*
: Legt den Pfad und den Dateinamen für die Pufferdateien fest. Die Standardeinstellung ist `/var/nfs/nfslog_workbuffer`.

logformat=*basic*|*extended*
: Legt das Format fest, das verwendet wird, um vom Benutzer lesbare Protokolldateien zu erstellen. Aus dem Basisformat resultiert eine Protokolldatei, die Ähnlichkeit mit manchen `ftpd`-Dämonen hat. Das erweiterte Format bietet eine detailliertere Ansicht.

Wenn kein Pfad angegeben ist, wird der durch `defaultdir` definierte Pfad verwendet. Außerdem können Sie `defaultdir` außer Kraft setzen, indem Sie einen absoluten Pfad angeben.

Um die Dateien einfacher zuordnen zu können, legen Sie sie in separaten Verzeichnissen ab. Es folgt ein Beispiel für erforderliche Änderungen:

```
% cat /etc/nfs/nfslog.conf
#ident  "@(#)nfslog.conf        1.5     99/02/21 SMI"
#
  .
  .
# NFS server log configuration file.
#

global  defaultdir=/var/nfs \
        log=nfslog fhtable=fhtable buffer=nfslog_workbuffer

publicftp log=logs/nfslog fhtable=fh/fhtables buffer=buffers/workbuffer
```

In diesem Beispiel werden in jedem Dateisystem, das mit `log=publicftp` gemeinsam genutzt wird, die folgenden Werte verwendet:

- Das Standardverzeichnis ist `/var/nfs`.
- Protokolldateien werden in `/var/nfs/logs/nfslog*` gespeichert.

- Dateizugriffsroutine-zu-Pfad-Datenbanktabellen werden in `/var/nfs/fh/fhtables` gespeichert.
- Pufferdateien werden in `/var/nfs/buffers/workbuffer` gespeichert.

Informationen zur Verfahrensweise finden Sie unter „So aktivieren Sie die NFS-Serverprotokollierung“ auf Seite 89.

NFS-Dämonen

Zur Unterstützung von NFS-Vorgängen werden verschiedene Dämonen gestartet, wenn ein System auf die Betriebsebene `3` oder in den Mehrbenutzermodus wechselt. Die Dämonen `mountd` und `nfsd` werden auf Systemen ausgeführt, bei denen es sich um Server handelt. Ob die Serverdämonen automatisch gestartet werden, hängt davon ab, ob Einträge vorhanden sind, die durch den NFS-Dateisystemtyp in `/etc/dfs/sharetab` gekennzeichnet sind. Zur Unterstützung der NFS-Dateisperrung werden die Dämonen `lockd` und `statd` auf NFS-Clients und -Servern ausgeführt. Anders als in den NFS-Vorgängerversionen werden in NFS-Version 4 die Dämonen `lockd`, `statd`, `mountd` und `nfslogd` nicht verwendet.

In diesem Abschnitt werden die folgenden Dämonen beschrieben:

- „`automountd`-Dämon“ auf Seite 147
- „`lockd`-Dämon“ auf Seite 148
- „`mountd`-Dämon“ auf Seite 149
- „`nfs4cbd`-Dämon“ auf Seite 149
- „`nfsd`-Dämon“ auf Seite 150
- „`nfslogd`-Dämon“ auf Seite 150
- „`nfsmapid`-Dämon“ auf Seite 151
- „`statd`-Dämon“ auf Seite 159

`automountd`-Dämon

Dieser Dämon verarbeitet Ein- und Aushängungsanforderungen des autofs-Service. Die Syntax des Befehls lautet folgendermaßen:

`automountd [ -Tnv ] [ -D` *name*`=` *value* `]`

Der Befehl bewirkt Folgendes:

- `-T` aktiviert die Ablaufverfolgung.
- `-n` deaktiviert Suchvorgänge auf allen autofs-Knoten.
- `-v` protokolliert alle Statusmeldungen auf der Konsole.
- `-D` *name*=*value* ersetzt *value* für die Variable der automount-Map, die durch *name* angegeben ist.

Der Standardwert für die automount-Map ist `/etc/auto_master`. Verwenden Sie die Option `-T` zur Fehlerbehebung.

`lockd`-Dämon

Dieser Dämon unterstützt Datensatzsperrvorgänge für NFS-Dateien. Der `lockd`-Dämon steuert RPC-Verbindungen zwischen Client und Server für das NLM-Protokoll (Network Lock Manager). Der Dämon wird normalerweise ohne Optionen gestartet. Sie können drei Optionen in Verbindung mit diesem Befehl angeben. Weitere Informationen finden Sie auf der Manpage `lockd(1M)`. Diese Optionen können entweder über die Befehlszeile oder durch Bearbeiten der entsprechenden Zeichenfolge in `/etc/default/nfs` verwendet werden. Es folgen Beschreibungen von Schlüsselwörtern, die in der `/etc/default/nfs`-Datei angegeben werden können.

Hinweis – Ab Solaris 10 werden das Schlüsselwort `LOCKD_GRACE_PERIOD` und die Option `-g` nicht mehr verwendet. Das veraltete Schlüsselwort wird durch das neue Schlüsselwort `GRACE_PERIOD` ersetzt. Wenn beide Schlüsselwörter angegeben sind, setzt der Wert für `GRACE_PERIOD` den Wert für `LOCKD_GRACE_PERIOD` außer Kraft. Weitere Informationen finden Sie in der folgenden Beschreibung von `GRACE_PERIOD`.

Ebenso wie bei `LOCKD_GRACE_PERIOD` , `GRACE_PERIOD`=*graceperiod* in `/etc/default/nfs` wird die Zeit (in Sekunden) nach einem Serverneustart festgelegt, nach deren Verstreichen die Clients sowohl die von NLM bereitgestellten Sperren der NFS-Version 3 als auch die Sperren der Version 4 zurückfordern müssen. Der Wert `GRACE_PERIOD` bestimmt damit die Länge der Wartezeit für die Wiederherstellung der Sperre für NFS-Versionen 3 und 4.

Der `LOCKD_RETRANSMIT_TIMEOUT`=*timeout*-Parameter in `/etc/default/nfs` gibt die Dauer der Wartezeit in Sekunden an, bevor eine Sperranforderung erneut an den Remote-Server gesendet wird. Diese Option wirkt sich auf den clientseitigen NFS-Service aus. Der Standardwert für *timeout* beträgt 15 Sekunden. Durch eine Herabsetzung des *timeout*-Werts kann die Reaktionszeit für NFS-Clients in einem Netzwerk mit starker Aktivität verbessert werden. Diese Änderung kann jedoch zu einer zusätzlichen Serverbelastung aufgrund von häufigeren Sperranforderungen führen. Der gleiche Parameter kann über die Befehlszeile angegeben werden, indem der Dämon mit der Option `-t` *timeout* gestartet wird.

Der `LOCKD_SERVERS`= *nthreads*-Parameter in `/etc/default/nfs` gibt die maximale Anzahl von gleichzeitig aktiven Threads an, die vom Server pro Verbindung verarbeitet werden. Geben Sie den Wert *nthreads* unter Berücksichtigung der erwarteten Belastung des NFS-Servers an. Der Standardwert ist 20. Jeder NFS-Client, der TCP verwendet, verwendet eine einzelne Verbindung mit dem NFS-Server. Darum kann jeder Client maximal 20 gleichzeitig aktive Threads auf dem Server verwenden.

Alle NFS-Clients, die UDP verwenden, verwenden gemeinsam eine einzelne Verbindung mit dem NFS-Server. Unter diesen Bedingungen müssen Sie eventuell die Anzahl der Threads erhöhen, die für die UDP-Verbindung zur Verfügung stehen. Es müssen mindestens zwei Threads für jeden UDP-Client bereitgestellt werden. Da sich dies jedoch auf die Arbeitslast auf dem Client bezieht, reichen zwei Threads pro Client unter Umständen nicht aus. Der Nachteil der Verwendung von mehreren Threads ist, dass mehr Speicherplatz auf dem NFS-Server belegt wird. Wenn die Threads jedoch nicht verwendet werden, ist die Erhöhung von *nthreads* bedeutungslos. Der gleiche Parameter kann über die Befehlszeile wirksam werden, wenn der Dämon mit der Option `nthreads` gestartet wird.

`mountd`-Dämon

Dieser Dämon verarbeitet von Remote-Systemen eingehende Anforderungen für die Einhängung von Dateisystemen und sorgt für die Zugriffssteuerung. Der `mountd`-Dämon prüft `/etc/dfs/sharetab`, um festzustellen, welche Dateisysteme für die Remote-Einhängung zur Verfügung stehen und welchen Systemen erlaubt ist, Remote-Einhängungen durchzuführen. Sie können die Optionen `-v` und `-r` in Verbindung mit diesem Befehl verwenden. Weitere Informationen finden Sie auf der Manpage `mountd(1M)`.

Die Option `-v` bewirkt, dass der Befehl im ausführlichen Modus ausgeführt wird. Jedesmal, wenn ein NFS-Server bestimmt, welchem Client der Zugriff gewährt werden soll, wird auf der Konsole eine Meldung ausgegeben. Die generierten Informationen können hilfreich sein, wenn versucht wird, die Ursache festzustellen, warum ein Client nicht auf ein Dateisystem zugreifen kann.

Die Option `-r` bewirkt, dass alle weiteren Einhängungsanforderungen, die von den Clients kommen, abgewiesen werden. Diese Option hat keinen Einfluss auf Clients, bei denen bereits ein Dateisystem eingehängt ist.

Hinweis – In NFS-Version 4 wird dieser Dämon nicht verwendet.

`nfs4cbd`-Dämon

Der Dämon `nfs4cbd`, der ausschließlich für die Verwendung des Clients der NFS-Version 4 bestimmt ist, verwaltet die Kommunikationsendpunkte für das Callback-Programm von NFS-Version 4. Der Dämon besitzt keine für den Benutzer zugängliche Schnittstelle. Weitere Informationen finden Sie auf der Manpage `nfs4cbd(1M)`.

nfsd-Dämon

Dieser Dämon bearbeitet sonstige Clientdateisystemanforderungen. Sie können mehrere Optionen in Verbindung mit diesem Befehl verwenden. Ein vollständige Liste finden Sie auf der Manpage nfsd(1M). Diese Optionen können entweder über die Befehlszeile oder durch Bearbeiten der entsprechenden Zeichenfolge in /etc/default/nfs verwendet werden.

Der NFSD_LISTEN_BACKLOG=*length*-Parameter in /etc/default/nfs dient zur Festlegung der Länge der Verbindungswarteschlange bei verbindungsorientierten Übertragungen für NFS und TCP. Der Standardwert ist 32 Einträge. Dieselbe Auswahl kann über die Befehlszeile vorgenommen werden, indem nfsd mit der Option -l gestartet wird.

Der NFSD_MAX_CONNECTIONS=*#-conn*-Parameter in /etc/default/nfs dient zur Auswahl der maximalen Anzahl von Verbindungen pro verbindungsorientierte Übertragung. Der Standardwert für *#-conn* ist unbegrenzt. Der gleiche Parameter kann über die Befehlszeile angegeben werden, indem der Dämon mit der Option -c *#-conn* gestartet wird.

Der NFSD_SERVER=*nservers*-Parameter in /etc/default/nfs dient zur Auswahl der maximalen Anzahl von gleichzeitigen Anforderungen, die von einem Server verarbeitet werden können. Der Standardwert für *nservers* ist 16. Dieselbe Auswahl kann über die Befehlszeile vorgenommen werden, indem nfsd mit der Option nservers gestartet wird.

Anders als bei älteren Versionen dieses Dämons produziert nfsd nicht mehrere Instanzen, damit gleichzeitige Anforderungen verarbeitet werden können. Eine Prüfung der Verarbeitungstabelle mit ps zeigt, dass nur eine Instanz des Dämons ausgeführt wird.

nfslogd-Dämon

Dieser Dämon sorgt für die Protokollierung von Vorgängen. Die Protokollierung serverbezogener NFS-Vorgänge basiert auf den Konfigurationsoptionen, die in /etc/default/nfslogd definiert sind. Wenn die NFS-Serverprotokollierung aktiviert ist, werden die Datensätze, in denen alle in einem bestimmten Dateisystem ausgeführten RPC-Vorgänge erfasst sind, vom Kernel in eine Pufferdatei geschrieben. Dann führt nfslogd eine Nachverarbeitung dieser Anforderungen aus. Der Name Service Switch wird verwendet, um UIDs den Anmeldungen und IP-Adressen für Hostnamen zuzuordnen. Der resultierende Wert wird aufgezeichnet, wenn keine Übereinstimmung durch die angegebenen Name Services festgestellt werden kann.

Die Zuordnung von Dateizugriffsroutinen zu Pfadnamen wird ebenfalls von nfslogd durchgeführt. Der Dämon verfolgt diese Zuordnungen in einer Dateizugriffsroutine-zu-Pfad-Map. Für jedes Tag, das in /etc/nfs/nfslogd angegeben ist, ist eine Map vorhanden. Nach der Nachverarbeitung werden die Datensätze in ASCII-Protokolldateien geschrieben.

Hinweis – In NFS-Version 4 wird dieser Dämon nicht verwendet.

`nfsmapid`-Dämon

In Version 4 des NFS-Protokolls (RFC3530) wurde die Art und Weise des Austauschs von Benutzer- oder Gruppen-IDs (UIDs oder GIDs) zwischen Client und Server geändert. Das Protokoll verlangt, dass die Eigentümer- und Gruppenattribute einer Datei zwischen einem Client der NFS-Version 4 und einem Server der NFS-Version 4 als Zeichenfolgen in der Form von `user@nfsv4_domain` bzw. `group@nfsv4_domain` ausgetauscht werden.

Der Benutzer `known_user` hat beispielsweise die UID 123456 auf einem Client der NFS-Version 4, dessen voll qualifizierter Hostname `system.example.com` lautet. Damit der Client Anforderungen an den Server der NFS-Version 4 senden kann, muss er die UID 123456 der E-Mail-Adresse `known_user@example.com` zuordnen und dieses Attribut dann an den Server der NFS-Version 4 senden. Der Server der NFS-Version 4 erwartet den Empfang von Benutzer- und Gruppendateiattributen im `user_or_group@nfsv4_domain` -Format. Nachem der Server `known_user@example.com` vom Client empfangen hat, ordnet er die Zeichenfolge der lokalen UID 123456 zu, was vom zugrunde liegenden Dateisystem verstanden wird. Diese Funktionsweise setzt voraus, dass jede UID und GID im Netzwerk eindeutig ist und die Domains der NFS-Version 4 auf dem Client mit den Domains der NFS-Version 4 auf dem Server übereinstimmen.

Hinweis – Wenn der Server nicht den angegebenen Benutzer- oder Gruppennamen erkennt, kann er diesen nicht der entsprechenden eindeutigen ID zuordnen, die ein Ganzzahlwert ist. Dies ist auch dann der Fall, wenn die Domains der NFS-Version 4 übereinstimmen. In solch einem Fall ordnet der Server den eingehenden Benutzer- oder Gruppennamen dem Benutzer `nobody` zu. Um dies zu verhindern, sollten Administratoren die Verwendung spezieller Konten vermeiden, die nur auf dem Client der NFS-Version 4 vorhanden sind.

Der Client wie auch der Server der NFS-Version 4 sind in der Lage, Ganzzahlen in Zeichenfolgen und Zeichenfolgen in Ganzzahlen zu konvertieren. Wenn beispielsweise ein GETATTR-Vorgang stattgefunden hat, ordnet der Server der NFS-Version 4 die vom zugrunde liegenden Dateisystem kommenden UIDs und GIDs den entsprechenden Zeichenfolgen zu und sendet diese Informationen an den Client. Auch der Client muss UIDs und GIDs den Zeichenfolgen zuordnen. Wenn beispielsweise der Befehl `chown` ausgeführt wurde, ordnet der Client die neue UID oder GID einer Zeichenfolge zu, bevor er einen SETATTR-Vorgang an den Server sendet.

Beachten Sie jedoch, dass der Client und der Server unterschiedlich auf nicht bekannte Zeichenfolgen antwortet:

- Wenn der Benutzer nicht auf dem Server vorhanden ist, lehnt der Server den Remote-Prozeduraufruf (RPC) ab und gibt eine Fehlermeldung an den Client zurück. Dies geschieht selbst dann, wenn es sich um dieselbe Domainkonfiguration der NFS-Version 4 handelt. Dadurch werden die Vorgänge begrenzt, die vom Remote-Benutzer ausgeführt werden können.
- Wenn der Benutzer sowohl auf dem Client als auch auf dem Server vorhanden ist, aber die Domains nicht übereinstimmen, lehnt der Server die Attributänderungsvorgänge (wie beispielsweise SETATTR) ab, die von ihm verlangen, die eingehende Benutzer-Zeichenfolge einem Ganzzahlwert zuzuordnen, der vom zugrunde liegenden Dateisystem verstanden werden kann. Damit die Clients und Server der NFS-Version 4 richtig funktionieren, müssen ihre Domains der NFS-Version 4, d. h. der Teil der Zeichenfolge hinter dem `@`-Zeichen, übereinstimmen.
- Wenn der Client der NFS-Version 4 keinen Benutzer- oder Gruppennamen des Servers erkennt, kann der Client die Zeichenfolge nicht der entsprechenden eindeutigen ID zuordnen, die ein Ganzzahlwert ist. In solch einem Fall ordnet der Client die eingehende Benutzer- oder Gruppenzeichenfolge dem Benutzer `nobody` zu. Diese Zuordnung zu `nobody` führt zu diversen Problemen für verschiedene Anwendungen. Was die Funktionen von NFS-Version 4 anbetrifft, so können Vorgänge zum Modifizieren von Dateiattributen nicht erfolgreich ausgeführt werden.

Sie können den Domainnamen für die Clients und Server mithilfe des Befehls `sharectl` und mit der folgenden Option ändern.

nfsmapid_domain
: Legt eine allgemeine Domain für Clients und Server fest. Setzt die standardmäßige Verwendung des lokalen DNS-Domainnamens außer Kraft. Aufgabenbezogene Informationen finden Sie unter „Einrichten von NFS-Services“ auf Seite 96.

Konfigurationsdateien und `nfsmapid`

Im Folgenden wird beschrieben, wie der Dämon `nfsmapid` die Dateien `/etc/nsswitch.conf` und `/etc/resolv.conf` verwendet:

- `nfsmapid` verwendet standardmäßige Funktionen der C-Bibliothek, um Passwort- und Gruppeninformationen von Backend-Name Services anzufordern. Diese Name Services werden durch Einstellungen in der `/etc/nsswitch.conf`-Datei gesteuert. Änderungen an der `nsswitch.conf`-Datei wirken sich auf `nfsmapid` -Vorgänge aus. Weitere Informationen zur `nsswitch.conf`-Datei finden Sie auf der Manpage `nsswitch.conf(4)`.
- Um sicherzustellen, dass die Clients der NFS-Version 4 Dateisysteme von verschiedenen Domains einhängen können, verwendet `nfsmapid` die Konfiguration des DNS-TXT-Ressourcendatensatzes (RR), `_nfsv4idmapdomain` . Weitere Informationen zum Konfigurieren des `_nfsv4idmapdomain` -Ressourcendatensatzes finden Sie unter „`nfsmapid` und DNS-TXT-Datensätze“ auf Seite 154. Beachten Sie zudem Folgendes:
  - Der DNS-TXT-Ressourcendatensatz muss unter Angabe der entsprechenden Domaininformationen explizit auf dem DNS-Server konfiguriert sein.
  - Die `/etc/resolv.conf`-Datei sollte mit den entsprechenden Parametern konfiguriert werden, um dem `resolver` zu ermöglichen, den DNS-Server zu finden und nach den Textdatensätzen für die Domains der NFS-Version 4 des Clients und des Servers zu suchen.

  Weitere Informationen finden Sie hier:

  - „Vorrangsregeln“ auf Seite 153
  - „Konfigurieren der Standarddomain der NFS-Version 4“ auf Seite 156
  - Manpage `resolv.conf(4)`

Vorrangsregeln

Damit `nfsmapid` richtig funktioniert, müssen die Clients und Server der NFS-Version 4 dieselbe Domain haben. Um sicherzustellen, dass die Domains der NFS-Version 4 übereinstimmen, richtet sich `nfsmapid` nach den folgenden Vorrangsregeln:

1. Zunächst prüft der Dämon die Datei `/etc/default/nfs` auf einen Wert, der dem Schlüsselwort NFSMAPID_DOMAIN zugewiesen wurde. Falls ein solcher Wert gefunden wird, hat er Vorrang vor allen sonstigen Einstellungen. Der zugewiesene Wert wird an die abgehenden Attributzeichenfolgen angehängt und mit den eingehenden Attributzeichenfolgen verglichen. Weitere Informationen zu Schlüsselwörtern in der `/etc/default/nfs`-Datei finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144. Informationen zur Verfahrensweise finden Sie unter „Einrichten von NFS-Services“ auf Seite 96.

Hinweis – Die Verwendung der Einstellung NFSMAPID_DOMAIN ist nicht skalierbar und wird nicht für große Bereitstellungen empfohlen.

2. Falls dem Schlüsselwort NFSMAPID_DOMAIN kein Wert zugewiesen ist, sucht der Dämon nach einem Domainnamen in einem DNS-TXT-Ressourcendatensatz. `nfsmapid` verwendet die Anweisung in der `/etc/resolv.conf`-Datei, die von den Routinen im `resolver` verwendet werden. Der `resolver` durchsucht die konfigurierten DNS-Server nach dem `_nfsv4idmapdomain`-TXT-Ressourcendatensatz. Beachten Sie, dass die Verwendung von DNS-TXT-Ressourcendatensätzen skalierbarer ist. Aus diesem Grund ist die kontinuierliche Verwendung von TXT-Datensätzen der Angabe eines Schlüsselworts in der `/etc/default/nfs`-Datei vorzuziehen.
3. Wenn kein DNS-TXT-Datensatz konfiguriert ist, um einen Domainnamen bereitzustellen, verwendet der Dämon `nfsmapid` den Wert, der von der Anweisung `domain` oder `search` in der Datei `/etc/resolv.conf` angegeben wird, wobei die zuletzt angegebene Anweisung Priorität hat.

   Im folgenden Beispiel, in dem sowohl `domain`- als auch die `search`-Anweisung verwendet wird, verwendet der Dämon `nfsmapid` die erste Domain, die nach der `search`-Anweisung angegeben ist, d. h. `company.com`.

   ```
   domain example.company.com
   search company.com foo.bar.com
   ```
4. Wenn die Datei `/etc/resolv.conf` nicht vorhanden ist, ruft `nfsmapid` den Domainnamen der NFS-Version 4 ab, indem dem Verhalten des Befehls `domainname` gefolgt wird. Wenn die Datei `/etc/defaultdomain` vorhanden ist, verwendet `nfsmapid` den Inhalt der Datei für die Domain der NFS-Version 4. Wenn die Datei `/etc/defaultdomain` nicht vorhanden ist, verwendet `nfsmapid` den Domainnamen, der vom konfigurierten Naming Service des Netzwerks bereitgestellt wird. Weitere Informationen finden Sie auf der Manpage `domainname(1M)`.

`nfsmapid` und DNS-TXT-Datensätze

Da DNS überall zu finden ist, empfiehlt sich die Verwendung des Speicher- und Verteilungsmechanismus von DNS für den Domainnamen der NFS-Version 4. Aufgrund der natürlichen Skalierbarkeit von DNS ist die Verwendung von DNS-TXT-Ressourcendatensätzen zudem die bevorzugte Methode zum Konfigurieren des Domainnamens der NFS-Version 4 für große Bereitstellungen. Sie sollten den `_nfsv4idmapdomain`-TXT-Datensatz auf DNS-Servern der Unternehmensklasse konfigurieren. Durch eine solche Konfiguration wird sichergestellt, dass jeder Client oder Server der NFS-Version 4 die entsprechende Domain der NFS-Version 4 in einer DNS-Struktur finden kann.

Es folgt ein Beispiel für einen bevorzugten Eintrag zum Aktivieren des DNS-Servers für die Bereitstellung eines Domainnamens der NFS-Version 4:

```
_nfsv4idmapdomain        IN        TXT            "foo.bar"
```

In diesem Beispiel ist der Domainname, der konfiguriert werden soll, der Wert, der in Anführungszeichen eingeschlossen ist. Beachten Sie, dass kein `ttl`-Feld angegeben ist und dass keine Domain an `_nfsv4idmapdomain`, den Wert im `owner`-Feld, angefügt ist. Diese Konfiguration ermöglicht dem TXT-Datensatz, den `${ORIGIN}`-Eintrag der Zone aus dem SOA-Datensatz (Start-Of-Authority) zu verwenden. Wenn beispielsweise verschiedene Ebenen des Domain-Namespace vorhanden sind, kann der Datensatz folgendes Aussehen haben:

```
_nfsv4idmapdomain.subnet.yourcorp.com.    IN    TXT    "foo.bar"
_nfsv4idmapdomain.yourcorp.com.           IN    TXT    "foo.bar"
```

Diese Konfiguration bietet DNS-Clients zusätzliche Flexibilität bei der Verwendung der `resolv.conf`-Datei zum Durchsuchen der DNS-Baumstruktur. Weitere Informationen finden Sie auf der Manpage `resolv.conf(4)`. Dank dieser Funktion wird die Wahrscheinlichkeit erhöht, den TXT-Datensatz zu finden. DNS-Teildomains können ihre eigenen DNS-TXT-Ressourcendatensätze definieren, wodurch für noch größere Flexibilität gesorgt wird. Diese Fähigkeit ermöglicht DNS-Teildomains der unteren Ebene, den TXT-Datensatz außer Kraft zu setzen, der von der Domain der obersten Ebene definiert ist.

Hinweis – Die vom TXT-Datensatz angegebene Domain kann eine beliebige Zeichenfolge sein, die nicht unbedingt mit der DNS-Domain für Clients und Server übereinstimmen muss, die die NFS-Version 4 verwenden. Sie haben die Möglichkeit, Daten der NFS-Version 4 nicht für andere DNS-Domains freizugeben.

Ermitteln der Domain der NFS-Version 4

Bevor Sie einen Wert für die Domain der NFS-Version 4 Ihres Netzwerks zuweisen, prüfen Sie, ob bereits eine Domain der NFS-Version 4 für Ihr Netzwerk konfiguriert ist. In den folgenden Beispielen werden Möglichkeiten aufgezeigt, wie eine Domain der NFS-Version 4 in Ihrem Netzwerk ermittelt werden kann.

- Um die Domain der NFS-Version 4 anhand eines DNS-TXT-Ressourcendatensatz zu ermitteln, verwenden Sie entweder den Befehl `nslookup` oder den Befehl `dig`:

  Es folgt eine Beispielausgabe für den Befehl `nslookup`:

  ```
  # nslookup -q=txt _nfsv4idmapdomain
  Server:         10.255.255.255
  Address:        10.255.255.255#53

  _nfsv4idmapdomain.example.company.com text = "company.com"
  ```

  Dies ist eine Beispielausgabe für den Befehl `dig`:

  ```
  # dig +domain=example.company.com -t TXT _nfsv4idmapdomain
  ...
  ;; QUESTION SECTION:
  ;_nfsv4idmapdomain.example.company.com. IN    TXT
  ```

```
;; ANSWER SECTION:
_nfsv4idmapdomain.example.company.com. 21600 IN TXT   "company.com"

;; AUTHORITY SECTION:
...
```

Weitere Informationen zum Einrichten eines DNS-TXT-Ressourcendatensatzes finden Sie unter „nfsmapid und DNS-TXT-Datensätze“ auf Seite 154.

- Wenn Ihr Netzwerk nicht mit einem DNS-TXT-Ressourcendatensatz der NFS-Version 4 eingerichtet ist, verwenden Sie den folgenden Befehl, um Ihre Domain der NFS-Version 4 anhand des DNS-Domainnamens zu ermitteln:

  ```
  # egrep domain /etc/resolv.conf
  domain example.company.com
  ```

- Wenn die Datei `/etc/resolv.conf` nicht für die Bereitstellung eines DNS-Domainnamens für den Client konfiguriert ist, verwenden Sie den folgenden Befehl, um die Domain anhand der Domainkonfiguration der NFS-Version 4 des Netzwerks zu ermitteln:

  ```
  # cat /var/run/nfs4_domain
  company.com
  ```

- Wenn Sie einen anderen Naming Service wie beispielsweise NIS verwenden, verwenden Sie den folgenden Befehl, um die Domain für den Naming Service zu ermitteln, der für Ihr Netzwerk konfiguriert ist:

  ```
  # domainname
  it.example.company.com
  ```

Weitere Informationen finden Sie auf den folgenden Manpages :

- `nslookup`(1M)
- `dig`(1M)
- `resolv.conf`(4)
- `domainname`(1M)

Konfigurieren der Standarddomain der NFS-Version 4

In diesem Abschnitt wird beschrieben, wie das Netzwerk die entsprechende Standarddomain abruft:

- Informationen zu den neuesten Versionen finden Sie unter „Konfigurieren der Standarddomain der NFS-Version 4“ auf Seite 157.
- Informationen zur Anfangsversion von Solaris 10 finden Sie unter „Konfigurieren einer Standarddomain der NFS-Version 4 mit Solaris 10“ auf Seite 158.

Konfigurieren der Standarddomain der NFS-Version 4

In der Anfangsversion von Solaris 10 wurde die Domain während des ersten Systemneustarts nach der Installation des Betriebssystems definiert. In höheren Versionen wird die Domain der NFS-Version 4 während der Installation des Betriebssystems definiert. Um diese Funktion bereitzustellen, wurden die folgenden Funktionen hinzugefügt:

- Der Befehl `sysidtool` schließt das Programm `sysidnfs4` ein. Das Programm wird während des Installationsprozesses ausgeführt, um festzustellen, ob eine Domain der NFS-Version 4 für das Netzwerk konfiguriert wurde. Weitere Informationen finden Sie auf den Manpages `sysidtool(1M)` und `sysidnfs4(1M)`.
- Die `sysidcfg`-Datei hat ein neues Schlüsselwort, `nfs4_domain`. Dieses Schlüsselwort kann verwendet werden, um die Domain der NFS-Version 4 zu definieren. Beachten Sie, dass auch andere Schlüsselwörter in der `sysidcfg`-Datei definiert werden können. Weitere Informationen finden Sie auf der Manpage `sysidcfg(4)`.

Im Folgenden wird die Funktionsweise beschrieben:

1. Das Programm `sysidnfs4` prüft die Datei `/etc/.sysIDtool.state` , um festzustellen, ob eine Domain der NFS-Version 4 ermittelt wurde.
   - Wenn die Datei `.sysIDtool.state` zeigt, dass eine Domain der NFS-Version 4 für das Netzwerk konfiguriert wurde, führt das Programm `sysidnfs4` weitere Prüfungen durch. Es folgt ein Beispiel für eine `.sysIDtool.state`-Datei:

     ```
     1       # System previously configured?
     1       # Bootparams succeeded?
     1       # System is on a network?
     1       # Extended network information gathered?
     1       # Autobinder succeeded?
     1       # Network has subnets?
     1       # root password prompted for?
     1       # locale and term prompted for?
     1       # security policy in place
     1       # NFSv4 domain configured
     xterms
     ```

     Die `1`, die vor `# NFSv4 domain configured` steht, bedeutet, dass die Domain der NFS-Version 4 konfiguriert wurde.
   - Wenn die `.sysIDtool.state`-Datei zeigt, dass keine Domain der NFS-Version 4 für das Netzwerk konfiguriert wurde, muss das Programm `sysidnfs4` weitere Prüfungen durchführen. Es folgt ein Beispiel für eine `.sysIDtool.state`-Datei:

     ```
     1       # System previously configured?
     1       # Bootparams succeeded?
     1       # System is on a network?
     1       # Extended network information gathered?
     1       # Autobinder succeeded?
     1       # Network has subnets?
     1       # root password prompted for?
     1       # locale and term prompted for?
     1       # security policy in place
     ```

```
0       # NFSv4 domain configured
xterms
```

Die `0`, die vor `# NFSv4 domain configured` steht, weist darauf hin, dass keine Domain der NFS-Version 4 konfiguriert wurde.

2. Wenn keine Domain der NFS-Version 4 ermittelt wurde, prüft das Programm `sysidnfs4` das `nfs4_domain`-Schlüsselwort in der `sysidcfg`-Datei.
   - Wenn ein Wert für `nfs4_domain` vorhanden ist, wird er dem Schlüsselwort NFSMAPID_DOMAIN in der `/etc/default/nfs`-Datei zugewiesen. Beachten Sie, dass jeder Wert, der NFSMAPID_DOMAIN zugewiesen ist, die Fähigkeit des Dämons `nfsmapid` außer Kraft setzt, Domains dynamisch auszuwählen. Weitere Informationen zur Funktion der Domains zur dynamischen Auswahl des Dämons `nfsmapid` finden Sie unter „Vorrangsregeln“ auf Seite 153.
   - Wenn kein Wert für `nfs4_domain` vorhanden ist, ermittelt das Programm `sysidnfs4` die Domain, die `nfsmapid` aus den konfigurierten Name Services des Betriebssystems ableitet. Dieser abgeleitete Wert wird als Standarddomain an einer interaktiven Eingabeaufforderung dargestellt, die Ihnen die Möglichkeit gibt, den Standardwert zu übernehmen oder eine andere Domain der NFS-Version 4 zuzuweisen.

Dadurch wird Folgendes nicht mehr benötigt:

- Das im Beispiel angeführte JumpStart-Skript `set_nfs4_domain` der Anfangsversion von Solaris 10 wird nicht mehr benötigt. Von einer weiteren Verwendung wird abgeraten.
- Die `/etc/.NFS4inst_state.domain`-Datei, die durch die frühere Implementierung des `sysidnfs4`-Programms erstellt wurde, wird nicht mehr benötigt.

Hinweis – Aufgrund der Allgegenwärtigkeit und natürlichen Skalierbarkeit von DSN werden DNS-TXT-Datensätze zum Konfigurieren der Domain von großen Bereitstellungen der NFS-Version 4 weiterhin bevorzugt verwendet. Dies wird auch nachdrücklich empfohlen. Lesen Sie dazu auch „`nfsmapid` und DNS-TXT-Datensätze“ auf Seite 154.

Ausführliche Informationen zum Solaris-Installationsprozess finden Sie hier:

- *Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen*
- *Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation*

Konfigurieren einer Standarddomain der NFS-Version 4 mit Solaris 10

Wenn Sie die NFS-Version der Anfangsversion von Solaris 10 verwenden und Ihr Netzwerk mehrere DNS-Domains, aber nur einen einzelnen UID- und GID-Namespace umfasst, müssen alle Clients den gleichen Wert für NFSMAPID_DOMAIN verwenden. Bei Standorten, die DNS verwenden, löst `nfsmapid` dieses Problem, indem der Domainname aus dem Wert abgerufen wird, den Sie `_nfsv4idmapdomain` zugewiesen haben. Weitere Informationen finden Sie unter

„nfsmapid und DNS-TXT-Datensätze“ auf Seite 154. Wenn Ihr Netzwerk nicht zur Verwendung von DNS konfiguriert ist, verwendet das Betriebssystem beim ersten Starten des Systems das Dienstprogramm sysidconfig(1M), um folgende Eingabeaufforderungen für einen Domänennamen der NFS-Version 4 bereitzustellen:

```
This system is configured with NFS version 4, which uses a
domain name that is automatically derived from the system's
name services. The derived domain name is sufficient for most
configurations. In a few cases, mounts that cross different
domains might cause files to be owned by nobody due to the
lack of a common domain name.

Do you need to override the system's default NFS verion 4 domain
name (yes/no)? [no]
```

Die Standardantwort ist [no]. Wenn Sie [no] wählen, wird Folgendes angezeigt:

```
For more information about how the NFS version 4 default domain name is
derived and its impact, refer to the man pages for nfsmapid(1M) and
nfs(4), and the System Administration Guide: Network Services.
```

Wenn Sie [yes] wählen, wird die folgende Eingabeaufforderung angezeigt:

```
Enter the domain to be used as the NFS version 4 domain name.
NFS version 4 domain name []:
```

Hinweis – Wenn ein Wert für NFSMAPID_DOMAIN in /etc/default/nfs vorhanden ist, setzt der von Ihnen angegebene [domain_name] den Wert außer Kraft.

Zusätzliche Informationen zu nfsmapid

Weitere Informationen zu nfsmapid finden Sie hier:

- Manpage nfsmapid(1M)
- Manpage nfs(4)
- http://www.ietf.org/rfc/rfc1464.txt
- „Zugriffskontrolllisten (ACLs) und nfsmapid in NFS-Version 4“ auf Seite 197

statd-Dämon

Dieser Dämon stellt in Verbindung mit lockd Funktionen zur Wiederherstellung nach einem Systemabsturz für den Sperren-Manager bereit. Der statd-Dämon verfolgt die Clients, die über Sperren auf einem NFS-Server verfügen. Wenn ein Server abstürzt, kontaktiert der auf dem Server befindliche Dämon statd während des Neustarts den auf dem Client befindlichen Dämon statd. Der Client statd kann versuchen, Sperren auf dem Server zurückzufordern. Der Client statd benachrichtigt zudem den Server statd, wenn ein Client abgestützt ist, damit

die Sperren des Clients auf dem Server entfernt werden können. Für diesen Dämon stehen keine Auswahloptionen zur Verfügung. Weitere Informationen finden Sie auf der Manpage `statd(1M)`.

In Solaris 7 wurde das Verfahren zum Verfolgen des Clients mit `statd` verbessert. In allen früheren Solaris-Versionen hat `statd` mithilfe des nicht qualifizierten Hostnamens für jeden Client Dateien in `/var/statmon/sm` erstellt. Die Dateibenennung verursachte Probleme, wenn zwei Clients mit demselben Hostnamen in verschiedenen Domains vorhanden waren oder wenn sich Clients nicht in derselben Domain wie der NFS-Server befanden. Da durch den nicht qualifizierten Hostnamen nur der Hostname (ohne Informationen zur Domain oder IP-Adresse) angegeben wird, konnte mit der älteren Version von `statd` nicht zwischen Clients unterschieden werden. Um dieses Problem zu beheben, erstellt der Dämon `statd` von Solaris 7 eine symbolische Verknüpfung in `/var/statmon/sm` mit dem nicht qualifizierten Hostnamen her, indem die IP-Adresse des Clients verwendet wird. Die neue Verknüpfung sieht wie folgt aus:

```
# ls -l /var/statmon/sm
lrwxrwxrwx   1 daemon          11 Apr 29 16:32 ipv4.192.168.255.255 -> myhost
lrwxrwxrwx   1 daemon          11 Apr 29 16:32 ipv6.fec0::56:a00:20ff:feb9:2734 -> v6host
--w-------   1 daemon          11 Apr 29 16:32 myhost
--w-------   1 daemon          11 Apr 29 16:32 v6host
```

In diesem Beispiel lautet der Hostname des Clients `myhost`, und die IP-Adresse des Clients lautet `192.168.255.255`. Wenn ein anderer Host mit dem Namen `myhost` ein Dateisystem erstellt, verweisen zwei symbolische Verknüpfungen auf den Hostnamen.

Hinweis – In NFS-Version 4 wird dieser Dämon nicht verwendet.

NFS-Befehle

Diese Befehle müssen von einem `root`-Benutzer ausgeführt werden, damit sie vollständig wirksam sind, aber Informationen können von allen Benutzern angefordert werden:

- „`automount`-Befehl“ auf Seite 161
- „`clear_locks`-Befehl“ auf Seite 161
- „`fsstat`-Befehl“ auf Seite 162
- „`mount`-Befehl“ auf Seite 162
- „`mountall`-Befehl“ auf Seite 170
- „`setmnt`-Befehl“ auf Seite 179
- „`share`-Befehl“ auf Seite 171
- „`shareall`-Befehl“ auf Seite 177
- „`showmount`-Befehl“ auf Seite 178
- „`umount`-Befehl“ auf Seite 169
- „`umountall`-Befehl“ auf Seite 170
- „`unshare`-Befehl“ auf Seite 177

- „unshareall-Befehl“ auf Seite 178

automount-Befehl

Dieser Befehl dient zum Installieren von autofs-Einhängepunkten und zum Zuordnen der Informationen in den automaster-Dateien zu jedem Einhängepunkt. Die Syntax des Befehls lautet folgendermaßen:

`automount [ -t` *duration* `] [ -v ]`

`-t` *duration* dient zum Festlegen der Zeitspanne in Sekunden, in der ein Dateisystem eingehängt bleiben soll, und `-v` dient zur Auswahl des ausführlichen Modus. Wenn dieser Befehl im ausführlichen Modus ausgeführt wird, ist eine einfachere Fehlerbehebung möglich.

Wenn keine Einstellung vorgenommen wird, wird die Zeitspanne auf fünf Minuten gesetzt. In den meisten Fällen ist dieser Wert angemessen. Bei Systemen mit vielen automatisch eingehängten Dateisystemen müssen Sie den Wert jedoch eventuell erhöhen. Vor allem kann es ineffzient sein, die automatisch eingehängten Dateisysteme alle fünf Minuten zu prüfen, wenn ein Server viele aktive Benutzer hat. Es empfiehlt sich darum, die autofs-Dateisysteme alle 1800 Sekunden (30 Minuten) zu prüfen. Wenn die Dateisysteme nicht alle fünf Minuten ausgehängt werden, kann `/etc/mnttab` bedeutend an Größe zunehmen. Um die Ausgabe zu verringern, wenn `df` jeden Eintrag `/etc/mnttab` prüft, können Sie die Ausgabe von `df` filtern, indem Sie die Option `-F` verwenden (siehe Manpage `df(1M)`), oder indem Sie `egrep` verwenden.

Sie sollten berücksichtigen, dass die Anpassung dieser Zeitspanne sich auch darauf auswirkt, wie schnell die Änderungen an den Automounter-Maps an anderer Stelle reflektiert werden. Die Änderungen sind erst dann sichtbar, wenn das Dateisystem ausgehängt ist. Anweisungen zum Modifizieren von Automounter-Maps finden Sie unter „Modifizieren der Maps“ auf Seite 111.

clear_locks-Befehl

Mithilfe dieses Befehls können Sie alle Datei- und Datensatzsperren sowie Sperren der gemeinsamen Nutzung für einen NFS-Client aufheben. Sie müssen als `root`-Benutzer angemeldet sein, um diesen Befehl auszuführen. Von einem NFS-Server aus können Sie die Sperren für einen bestimmten Client aufheben. Von einem NFS-Client aus können Sie die Sperren für diesen Client auf einem bestimmten Server aufheben. Im folgenden Beispiel werden die Sperren für einen NFS-Client namens `tulip` im aktuellen System aufgehoben.

```
# clear_locks tulip
```

Mithilfe der Option `-s` können Sie angeben, von welchem NFS-Host die Sperren entfernt werden sollen. Sie müssen diese Option von dem NFS-Client aus ausführen, der die Sperren aktiviert hat. In diesem Fall werden die Sperren des Clients von dem NFS-Server namens `bee` entfernt.

```
# clear_locks -s bee
```

Achtung – Dieser Befehl sollte nur dann ausgeführt werden, wenn ein Client abgestürzt ist und seine Sperren nicht entfernen kann. Um Probleme durch Datenbeschädigung zu vermeiden, sollten Sie keine Sperren entfernen, die für einen aktiven Client bestimmt sind.

`fsstat`-Befehl

Ab Solaris 10 11/06 können Sie das `fsstat`-Dienstprogramm verwenden, um Dateisystemvorgänge nach Dateisystem und Einhängepunkt zu überwachen. Es stehen verschiedene Optionen zum Anpassen der Ausgabe zur Verfügung. Betrachten Sie hierzu folgende Beispiele.

Dieses Beispiel zeigt die Ausgabe der NFS-Versionen 3 und 4 und des `root`-Einhängepunkts.

```
% fsstat nfs3 nfs4 /
  new     name   name    attr    attr   lookup   rddir   read   read   write   write
 file    remov   chng     get     set     ops     ops    ops  bytes    ops   bytes
3.81K      90  3.65K   5.89M   11.9K    35.5M   26.6K   109K   118M   35.0K   8.16G  nfs3
  759     503    457   93.6K   1.44K     454K   8.82K  65.4K   827M     292    223K  nfs4
25.2K   18.1K  1.12K   54.7M    1017     259M   1.76M  22.4M  20.1G   1.43M   3.77G  /
```

In diesem Beispiel wird die Option `-i` verwendet, um Statistiken zu den E/A-Vorgängen für die NFS-Versionen 3 und 4 und zum `root`-Einhängepunkt bereitzustellen.

```
% fsstat -i nfs3 nfs4 /
 read    read    write   write   rddir   rddir   rwlock   rwulock
  ops   bytes      ops   bytes     ops   bytes      ops       ops
 109K    118M    35.0K   8.16G   26.6K   4.45M     170K      170K  nfs3
65.4K    827M      292    223K   8.82K   2.62M    74.1K     74.1K  nfs4
22.4M   20.1G    1.43M   3.77G   1.76M   3.29G    25.5M     25.5M  /
```

In diesem Beispiel wird die Option `-i` verwendet, um Statistiken zu den Naming-Vorgängen für die NFS-Versionen 3 und 4 und zum `root`-Einhängepunkt bereitzustellen.

```
% fsstat -n nfs3 nfs4 /
lookup   creat   remov  link   renam  mkdir  rmdir   rddir  symlnk  rdlnk
 35.5M   3.79K      90     2   3.64K      5      0   26.6K      11   136K  nfs3
  454K     403     503     0     101      0      0   8.82K     356  1.20K  nfs4
  259M   25.2K   18.1K   114    1017     10      2   1.76M      12  8.23M  /
```

Weitere Informationen finden Sie auf der Manpage `fsstat(1M)`.

`mount`-Befehl

Mit diesem Befehl können Sie ein benanntes lokales oder Remote-Dateisystem an einen bestimmten Einhängepunkt anfügen. Weitere Informationen finden Sie auf der Manpage

mount(1M). Wenn mount ohne Argumente verwendet wird, wird eine Liste von Dateisystemen angezeigt, die derzeit auf Ihrem Computer eingehängt sind.

In der standardmäßigen Solaris-Installation sind viele Dateisystemtypen enthalten. Für jeden Dateisystemtyp steht eine Manpage zur Verfügung, auf der die Optionen für mount aufgelistet sind, die für diesen Dateisystemtyp vorgesehen sind. Die Manpage für NFS-Dateisysteme ist mount_nfs(1M). Informationen zu UFS-Dateisystemen finden Sie auf der Manpage mount_ufs(1M).

Mit Solaris 7 kann ein Pfadname ausgewählt werden, um Einhängungen von einem NFS-Server aus auszuführen. Zu diesem Zweck wird eine NFS-URL anstelle der standardmäßigen server:/pathname -Syntax verwendet. Weitere Informationen finden Sie unter „So hängen Sie ein NFS-Dateisystem mithilfe einer NFS-URL ein“ auf Seite 95.

Achtung – Bei Verwendung der Version des Befehls mount wird nicht vor ungültigen Optionen gewarnt. Bei Verwendung des Befehls werden stillschweigend alle Optionen ignoriert, die nicht interpretiert werden können. Überprüfen Sie alle verwendeten Optionen, um ein unerwartetes Verhalten zu vermeiden.

mount-Optionen für NFS-Dateisysteme

Im nachfolgenden Text werden einige der Optionen aufgelistet, die hinter dem Flag -o stehen können, wenn Sie ein NFS-Dateisystem einhängen. Eine vollständige Liste der Optionen finden Sie auf der Manpage mount_nfs(1M).

bg|fg
: Diese Optionen können verwendet werden, um das Verhalten festzulegen, das für erneute Versuche gilt, wenn eine Einhängung fehlschlägt. Die Option bg bewirkt, dass Einhängeversuche im Hintergrund ausgeführt werden. Die Option fg bewirkt, dass Einhängeversuche im Vordergrund ausgeführt werden. Die Standardeinstellung fg eignet sich bestens für Dateisysteme, die verfügbar sein müssen. Diese Option verhindert eine weitere Verarbeitung, bis die Einhängung abgeschlossen ist. bg eignet sich für nicht kritische Dateisysteme, da der Client andere Verarbeitungsaufgaben ausführen kann, während auf den Abschluss der Verarbeitung der Einhängungsanforderung gewartet wird.

forcedirectio
: Mit dieser Option wird die Leistung von umfangreichen sequentiellen Datenübertragungen verbessert. Die Daten werden direkt in einen Benutzerpufferspeicher kopiert. Im Kernel auf dem Client findet keine Zwischenspeicherung statt. Diese Option ist standardmäßig deaktiviert.

  Zuvor wurden sämtliche Schreibzugriffsanforderungen sowohl vom NFS-Client als auch vom NFS-Server serialisiert. Der NFS-Client wurde dahin gehend verändert, dass Anwendungen gleichzeitige Schreibzugriffe sowie gleichzeitige Lese- und Schreibzugriffe auf eine einzige Datei durchführen können. Diese Funktion können Sie mit der Einhängeoption forcedirectio auf dem Client aktivieren. Durch Verwendung dieser

Option aktivieren Sie dieses Leistungsmerkmal für alle Dateien innerhalb des eingehängten Dateisystems. Über die Schnittstelle `directio()` können Sie das Leistungsmerkmal auch für eine gezielte Datei auf dem Client aktivieren. Solange diese Funktion nicht aktiviert ist, werden Schreibzugriffe auf Dateien serialisiert. Außerdem unterstützt eine Datei, auf die gleichzeitige Schreib- oder Lesezugriffe erfolgen, keine POSIX-Semantik mehr.

Ein Beispiel zur Verwendung dieser Option finden Sie unter „Verwenden des `mount`-Befehls“ auf Seite 167.

largefiles
: Mit dieser Option können Sie auf Dateien zugreifen, die größer als 2 GB sind. Da der Zugriff auf eine große Datei nur auf dem Server gesteuert werden kann, wird diese Option bei Einhängungen der NFS-Version 3 stillschweigend ignoriert. Alle UFS-Dateisysteme sind standardmäßig mit `largefiles` eingehängt. Bei Einhängungen mithilfe des Protokolls der NFS-Version 2 bewirkt die Option `largefiles`, dass die Einhängung fehlschlägt und ein Fehler gemeldet wird.

nolargefiles
: Diese Option für UFS-Einhängungen gewährleistet, dass keine großen Dateien im Dateisystem enthalten sind. Weitere Informationen finden Sie auf der Manpage `mount_ufs(1M)`. Da das Vorhandensein großer Dateien nur auf dem NFS-Server festgestellt werden kann, steht keine Option für `nolargefiles` zur Verfügung, wenn NFS-Einhängungen durchgeführt werden. Versuche, ein Dateisystem über NFS mit dieser Option einzuhängen, werden abgewiesen, und es wird ein Fehler ausgegeben.

nosuid|suid
: Ab Solaris 10 entspricht die Option `nosuid` der Angabe der Option `nodevices` in Verbindung mit der Option `nosetuid`. Wenn die Option `nodevices` angegeben ist, wird das Öffnen von gerätespezifischen Dateien auf dem eingehängten Dateisystem verweigert. Wenn die Option `nosetuid` angegeben ist, werden das `setuid`-Bit und das `setgid`-Bit, die sich in den Binärdateien des Dateisystems befinden, ignoriert. Die Prozesse werden mit den Berechtigungen des Benutzers ausgeführt, der die Binärdatei ausführt.

  Die Option `suid` entspricht der Angabe der Option `devices` in Verbindung mit der Option `setuid`. Wenn die Option `devices` angegeben ist, wird das Öffnen von gerätespezifischen Dateien auf dem eingehängten Dateisystem zugelassen. Wenn die Option `setuid` angegeben ist, werden das `setuid`-Bit und das `setgid`-Bit, die sich in den Binärdateien des Dateisystems befinden, vom Kernel akzeptiert.

  Wenn keine der Optionen angegeben ist, wird `suid` als standardmäßige Option verwendet, wodurch standardmäßig die Option `devices` in Verbindung mit der Option `setuid` verwendet wird.

  In der folgenden Tabelle wird das Verhalten beschrieben, das aus der Kombination von `nosuid` oder `suid` mit `devices` oder `nodevices` und `setuid` oder `nosetuid` resultiert. Beachten Sie, dass das Verhalten jeweils durch die kombinierte Option bestimmt wird, die mit den meisten Einschränkungen verbunden ist.

Verhalten, dass aus kombinierten Optionen resultiert	Option	Option	Option
Entspricht der Verwendung von `nosetuid` in Verbindung mit `nodevices`.	`nosuid`	`nosetuid`	`nodevices`
Entspricht der Verwendung von `nosetuid` in Verbindung mit `nodevices`.	`nosuid`	`nosetuid`	`devices`
Entspricht der Verwendung von `nosetuid` in Verbindung mit `nodevices`.	`nosuid`	`setuid`	`nodevices`
Entspricht der Verwendung von `nosetuid` in Verbindung mit `nodevices`.	`nosuid`	`setuid`	`devices`
Entspricht der Verwendung von `nosetuid` in Verbindung mit `nodevices`.	`suid`	`nosetuid`	`nodevices`
Entspricht der Verwendung von `nosetuid` in Verbindung mit `devices`.	`suid`	`nosetuid`	`devices`
Entspricht der Verwendung von `setuid` in Verbindung mit `nodevices`.	`suid`	`setuid`	`nodevices`
Entspricht der Verwendung von `setuid` in Verbindung mit `devices`.	`suid`	`setuid`	`devices`

Die Option `nosuid` bietet zusätzliche Sicherheit für NFS-Clients, die auf möglicherweise nicht vertrauenswürdige Server zugreifen. Das Einhängen von Remote-Dateisystemen mit dieser Option verringert die Wahrscheinlichkeit der Berechtigungseskalation durch nicht vertrauenswürdige Geräte oder nicht vertrauenswürdige `setuid`-Binärdateien. Alle diese Optionen sind in allen Solaris-Dateisystemen verfügbar.

public
: Mit dieser Option wird die Verwendung der Routine für den Zugriff auf öffentliche Dateien erzwungen, wenn der NFS-Server kontaktiert wird. Wenn die Routine für den Zugriff auf öffentliche Dateien durch den Server unterstützt wird, kann die Einhängung schneller durchgeführt werden, da das MOUNT-Protokoll nicht verwendet wird. Wenn das MOUNT-Protokoll nicht verwendet wird, gestattet die Option "public" zudem das Einhängen über eine Firewall.

rw|ro
: Mithilfe der Optionen `-rw` und `-ro` wird bestimmt, ob ein Dateisystem mit Lese- und Schreibzugriff oder mit Schreibschutz eingehängt wird. Die standardmäßig eingestellte Option für den Lese- und Schreibzugriff eignet sich für Remote-Home-Verzeichnisse, Mail-Spooling-Verzeichnisse oder andere Dateisysteme, die von Benutzern geändert werden müssen. Die Schreibschutz-Option eignet sich für Verzeichnisse, die nicht von Benutzern geändert werden sollten. Gemeinsam genutzte Kopien von Manpages sollten beispielsweise nicht von Benutzern beschrieben werden.

sec=*mode*
: Mithilfe dieser Option können Sie den Authentifizierungsmechanismus festlegen, der während der Einhängung verwendet werden soll. Folgende Werte für *mode* können verwendet werden:

  - Verwenden Sie `krb5` für den Authentifizierungsservice der Kerberos-Version 5.
  - Verwenden Sie `krb5i` für die Kerberos-Version 5 mit Integrität.
  - Verwenden Sie `krb5p` für die Kerberos-Version 5 mit Datenschutz.
  - Verwenden Sie `none`, wenn keine Authentifizierung durchgeführt werden soll.
  - Verwenden Sie `dh` für die DH-Authentifizierung (Diffie-Hellman).
  - Verwenden Sie `sys` für die standardmäßige UNIX-Authentifizierung.

  Die Modi sind auch in `/etc/nfssec.conf` definiert.

soft|hard
: Wenn ein NFS-Dateisystem mit der Option `soft` eingehängt wird, wird ein Fehler zurückgegeben, wenn der Server nicht antwortet. Die Option `hard` bewirkt, dass so lange versucht wird, die Einhängung durchzuführen, bis der Server antwortet. Die Standardeinstellung `hard` sollte für die meisten Dateisysteme verwendet werden. Anwendungen prüfen oft nicht die Rückgabewerte von Dateisystemen, die mit der Option `soft` eingehängt werden. Dies kann dazu führen, dass eine Anwendung ausfällt oder Dateien beschädigt werden. Selbst dann, wenn die Anwendung die Rückgabewerte prüft, können Routing-Probleme und andere Bedingungen die Anwendung irritieren oder zur Beschädigung von Dateien führen, wenn die Option `soft` verwendet wird. In den meisten Fällen sollte die Option `soft` nicht verwendet werden. Wenn ein Dateisystem mithilfe der Option `hard` eingehängt wird und dann nicht verfügbar ist, bleibt eine Anwendung, die dieses Dateisystem verwendet, hängen, bis das Dateisystem wieder verfügbar ist.

Verwenden des `mount`-Befehls

Die folgenden Beispiele dienen der Erläuterung.

- In NFS-Version 2 oder 3 wird ein NFS-Dateisystem des Servers bee mithilfe dieser Befehle mit Schreibschutz eingehängt.

  ```
  # mount -F nfs -r bee:/export/share/man /usr/man
  ```

  ```
  # mount -F nfs -o ro bee:/export/share/man /usr/man
  ```

  In NFS-Version 4 wird mithilfe der folgenden Befehlszeile dieselbe Einhängung durchgeführt:

  ```
  # mount -F nfs -o vers=4 -r bee:/export/share/man /usr/man
  ```

- In NFS-Version 2 oder 3 wird dieser Befehl in Verbindung mit der Option `-O` verwendet, um zu erzwingen, dass die Manpages des Servers bee auch dann auf dem lokalen System eingehängt werden, wenn `/usr/man` bereits eingehängt wurde. Siehe Folgendes:

  ```
  # mount -F nfs -O bee:/export/share/man /usr/man
  ```

  In NFS-Version 4 wird mithilfe der folgenden Befehlszeile dieselbe Einhängung durchgeführt:

  ```
  # mount -F nfs -o vers=4 -O bee:/export/share/man /usr/man
  ```

- In NFS-Version 2 oder 3 wird mithilfe dieses Befehls das Client-Failover verwendet.

  ```
  # mount -F nfs -r bee,wasp:/export/share/man /usr/man
  ```

  In NFS-Version 4 wird in der folgenden Befehlszeile das Client-Failover verwendet.

  ```
  # mount -F nfs -o vers=4 -r bee,wasp:/export/share/man /usr/man
  ```

  Hinweis – Bei Verwendung in der Befehlszeile müssen die aufgelisteten Server die gleiche Version des NFS-Protokolls unterstützen. Verwenden Sie die Server der Version 2 und 3 nicht gleichzeitig, wenn Sie `mount` über die Befehlszeile ausführen. Sie können beide Server in Verbindung mit autofs verwenden. Autofs wählt automatisch den geeignetsten der Server von Version 2 oder 3 aus.

- Es folgt ein Beispiel für die Verwendung einer NFS-URL mit dem Befehl `mount` in NFS-Version 2 oder 3.

  ```
  # mount -F nfs nfs://bee//export/share/man /usr/man
  ```

  Es folgt ein Beispiel für die Verwendung einer NFS-URL mit dem Befehl `mount` in NFS-Version 4.

  ```
  # mount -F nfs -o vers=4 nfs://bee//export/share/man /usr/man
  ```

- Verwenden Sie die Einhängeoption `forcedirectio`, damit der Client gleichzeitige Schreibzugriffe sowie gleichzeitige Lese- und Schreibzugriffe auf eine Datei zulässt. Es folgt ein Beispiel:

```
# mount -F nfs -o forcedirectio bee:/home/somebody /mnt
```

In diesem Beispiel wird mithilfe des Befehls eine NFS-Datei des Servers bee eingehängt. Außerdem werden gleichzeitige Lese- und Schreibzugriffe auf alle Dateien im Verzeichnis `/mnt` aktiviert. Wenn die Unterstützung für gleichzeitige Lese- und Schreibzugriffe aktiviert ist, geschieht Folgendes:

- Der Client lässt zu, dass eine Datei gleichzeitig durch mehrere Anwendungen beschrieben wird.
- Die Zwischenspeicherung auf dem Client wird deaktiviert. Dementsprechend bleiben die Daten, die aus den Lese- und Schreibzugriffen resultieren, auf dem Server. Da die Daten, die gelesen oder geschrieben wurden, also nicht vom Client zwischengespeichert werden, werden alle Daten, die noch nicht von der Anwendung selbst zwischengespeichert wurden, auf dem Server gelesen. Das Betriebssystem des Clients besitzt keine Kopie dieser Daten. Normalerweise werden die Daten vom NFS-Client im Kernel zwischengespeichert, damit diese von den Anwendungen verwendet werden können.

  Da die Zwischenspeicherung auf dem Client deaktiviert ist, sind somit auch das Vorauslesen und das verzögerte Schreiben deaktiviert. Ein Vorauslesevorgang findet statt, wenn der Kernel auf die Daten vorgreift, die voraussichtlich von einer Anwendung als Nächstes angefordert werden. Der Kernel beginnt dann, diese Daten im Voraus zu sammeln. Das Ziel des Kernels ist es, die Daten bereits bereitzuhalten, wenn diese von der Anwendung angefordert werden.

  Der Client verwendet den verzögerten Schreibvorgang, um die Schreibleistung zu erhöhen. Anstatt jedesmal einen E/A-Vorgang zu starten, wenn Daten von einer Anwendung in eine Datei geschrieben werden, werden die Daten zwischengespeichert. Später werden die Daten auf die Festplatte geschrieben.

  Durch den verzögerten Schreibvorgang können Daten in größeren Blöcken oder asynchron zur Anwendung geschrieben werden. Durch größere Blöcke wird die Schreibleistung erhöht. Asynchrone Schreibvorgänge gestatten die Überlagerung von Anwendungsprozessen und E/A-Prozessen. Außerdem erlauben asynchrone Schreibvorgänge dem Speicheruntersystem, die E/A-Prozesse zu optimieren, um für eine verbesserte sequentielle Verarbeitung der E/A-Prozesse zu sorgen. Durch synchrone Schreibvorgänge wird eine sequentielle Verarbeitung der E/A-Prozesse auf dem Speicheruntersystem erzwungen, die unter Umständen nicht optimal ist.
- Eine bedeutende Verschlechterung der Leistung kann eintreten, wenn die Anwendung nicht auf die Verarbeitung der Semantik der nicht zwischengespeicherten Daten vorbereitet ist. In Multithread-Anwendungen wird dieses Problem vermieden.

Hinweis – Wenn die Unterstützung für gleichzeitige Schreibvorgänge nicht aktiviert ist, werden alle Schreibanforderungen serialisiert. Wenn Anforderungen serialisiert werden, geschieht Folgendes: Wenn eine Schreibanforderung ausgeführt wird, wird die Verarbeitung einer weiteren Schreibanforderung erst dann fortgesetzt, wenn die Verarbeitung der ersten Schreibanforderung abgeschlossen ist.

- Verwenden Sie den Befehl `mount` ohne Argumente, um Dateisysteme anzuzeigen, die auf einem Client eingehängt sind. Siehe Folgendes:

```
% mount
/ on /dev/dsk/c0t3d0s0 read/write/setuid on Wed Apr 7 13:20:47 2004
/usr on /dev/dsk/c0t3d0s6 read/write/setuid on Wed Apr 7 13:20:47 20041995
/proc on /proc read/write/setuid on Wed Apr 7 13:20:47 2004
/dev/fd on fd read/write/setuid on Wed Apr 7 13:20:47 2004
/tmp on swap read/write on Wed Apr 7 13:20:51 2004
/opt on /dev/dsk/c0t3d0s5 setuid/read/write on Wed Apr 7 13:20:51 20041995
/home/kathys on bee:/export/home/bee7/kathys
  intr/noquota/nosuid/remote on Wed Apr 24 13:22:13 2004
```

`umount`-Befehl

Mithilfe dieses Befehls können Sie ein eingehängtes Remote-Dateisystem entfernen. Der Befehl `umount` unterstützt die Option `-V`, wodurch Prüfungen durchgeführt werden können. Sie können die Option `-a` auch verwenden, um mehrere Dateisysteme gleichzeitig auszuhängen. Wenn *mount-points* in die Option `-a` einbezogen sind, werden die betreffenden Dateisysteme ausgehängt. Wenn keine Einhängepunkte einbezogen sind, wird versucht, alle Dateisysteme auszuhängen, die in `/etc/mnttab` aufgelistet sind. Ausgenommen hiervon sind die erforderlichen Dateisysteme wie beispielsweise `/`, `/usr`, `/var`, `/proc`, `/dev/fd` und `/tmp`. Da das Dateisystem bereits eingehängt ist und ein dementsprechender Eintrag in `/etc/mnttab` vorhanden sein sollte, müssen Sie kein Flag für den Dateisystemtyp einfügen.

Die Option `-f` erzwingt das Aushängen eines ausgelasteten Dateisystems. Sie können diese Option verwenden, um einen Client auszuhängen, der bei dem Versuch hängen geblieben ist, ein nicht einhängbares Dateisystem einzuhängen.

Achtung – Wird das Aushängen eines Dateisystems erzwungen, können Datenverluste auftreten, wenn die Dateien während des Aushängens beschrieben werden.

Betrachten Sie hierzu folgende Beispiele.

BEISPIEL 6–1 Aushängen eines Dateisystems

In diesem Beispiel wird ein in `/usr/man` eingehängtes Dateisystem ausgehängt:

```
# umount /usr/man
```

BEISPIEL 6–2 Verwenden von Optionen in Verbindung mit `umount`

Dieses Beispiel zeigt die Ergebnisse der Ausführung des Befehls `umount -a -V`:

```
# umount -a -V
umount /home/kathys
umount /opt
umount /home
umount /net
```

Beachten Sie, dass die Dateisysteme durch diesen Befehl nicht ausgehängt werden.

`mountall`-Befehl

Verwenden Sie diesen Befehl, um alle Dateisysteme oder eine bestimmte Gruppe von Dateisystemen einzuhängen, die in der Dateisystemtabelle aufgelistet sind. Der Befehl kann für Folgendes verwendet werden:

- Auswählen des Dateisystemtyps, auf den mit der Option `-F` *FSType* zugegriffen wird
- Auswählen aller Remote-Dateisysteme, die in einer Dateisystemtabelle mit der Option `-r` aufgelistet werden
- Auswählen aller lokalen Dateisysteme mit der Option `-l`

Da alle als NFS-Dateisystemtyp bezeichneten Dateisysteme Remote-Dateisysteme sind, sind einige der genannten Optionen überflüssig. Weitere Informationen finden Sie auf der Manpage `mountall(1M)`.

Beachten Sie, dass die folgenden zwei Eingabebeispiele äquivalent sind:

```
# mountall -F nfs
```

```
# mountall -F nfs -r
```

`umountall`-Befehl

Verwenden Sie diesen Befehl, um eine Gruppe von Dateisystemen auszuhängen. Die Option `-k` dient zum Ausführen des `fuser -k` *-mount-point*-Befehls, durch den alle Prozesse abgebrochen werden, die mit dem *mount-point* verbunden sind. Die Option `-s` zeigt an, dass das Aushängen nicht parallel durchgeführt werden kann. `-l` gibt an, dass nur lokale Dateisysteme verwendet werden, und `-r` gibt an, dass nur Remote-Dateisysteme verwendet werden. Die Option `-h` *host* zeigt an, dass alle Dateisysteme des angegebenen Hosts ausgehängt werden sollen. Sie können die Option `-h` nicht mit `-l` oder `-r` kombinieren.

Es folgt ein Beispiel für die Aushängung aller eingehängten Dateisysteme von Remote-Hosts:

```
# umountall -r
```

Es folgt ein Beispiel für die Aushängung der gerade eingehängten Dateisysteme des Servers bee:

```
# umountall -h bee
```

share-Befehl

Mit diesem Befehl können Sie ein lokales Dateisystem auf einem NFS-Server für das Einhängen verfügbar machen. Außerdem können Sie den Befehl `share` verwenden, um eine Liste der Dateisysteme anzuzeigen, die derzeit auf Ihrem System gemeinsam genutzt werden. Der NFS-Server muss ausgeführt werden, damit der Befehl `share` funktioniert. Die NFS-Serversoftware wird automatisch während des Boot-Vorgangs gestartet, wenn ein entsprechender Eintrag in `/etc/dfs/dfstab` vorhanden ist. Nach Ausführung des Befehls wird kein Fehler gemeldet, wenn die NFS-Serversoftware nicht ausgeführt wird. Aus diesem Grund müssen Sie sicherstellen, dass die Software ausgeführt wird.

Zu den Objekten, die gemeinsam genutzt werden können, zählen Verzeichnisstrukturen. Jede Dateisystemhierarchie ist jedoch durch den Festplattenbereich oder die Partition beschränkt, auf der sich das Dateisystem befindet. Durch die gemeinsame Nutzung des Root-Dateisystems (`/`) wird beispielsweise das Verzeichnis `/usr` nicht gemeinsam genutzt, es sei denn, diese Verzeichnisse befinden sich auf derselben Festplattenpartition oder auf demselben Festplattenbereich. Bei der normalen Installation wird "root" auf den Bereich 0 und `/usr` auf den Bereich 6 gesetzt. Außerdem werden durch die gemeinsame Nutzung von `/usr` keine anderen lokalen Festplattenpartitionen gemeinsam genutzt, die in Unterverzeichnissen von `/usr` eingehängt sind.

Ein Dateisystem kann nicht gemeinsam genutzt werden, wenn es zu einem größeren Dateisystem gehört, das bereits gemeinsam genutzt wird. Wenn sich beispielsweise `/usr` und `/usr/local` auf einem Festplattenbereich befinden, kann `/usr` oder `/usr/local` gemeinsam genutzt werden. Wenn jedoch beide Dateisysteme mit unterschiedlichen Optionen zur gemeinsamen Nutzung bereitgestellt werden müssen, muss `/usr/local` auf einen separaten Festplattenbereich verschoben werden.

Sie können über die Dateizugriffsroutine eines gemeinsam genutzten Dateisystems mit Lese- und Schreibzugriff auf ein gemeinsam genutztes schreibgeschütztes Dateisystem zugreifen. Beide Dateisysteme müssen sich jedoch auf dem gleichen Festplattenbereich befinden. Sie können für mehr Sicherheit sorgen. Verschieben Sie die Dateisysteme, die lesbar und beschreibbar sein müssen, auf eine separate Partition oder einen separaten Festplattenbereich der Dateisysteme, die als schreibgeschützte Dateisysteme gemeinsam genutzt werden sollen.

Hinweis – Informationen zur Verhaltensweise der NFS-Version 4, die sich zeigt, wenn die gemeinsame Nutzung eines Dateisystems aufgehoben wird und das Dateisystem anschließend wieder gemeinsam genutzt wird, finden Sie unter „Aufheben der gemeinsamen Nutzung und erneutes Freigeben zur gemeinsamen Nutzung eines Dateisystems in NFS-Version 4“ auf Seite 188.

Nicht dateisystemspezifische `share`-Optionen

Es folgen einige der Optionen, die Sie zusammen mit dem Flag `-o` verwenden können:

rw|ro
: Das *pathname*-Dateisystem ist für die gemeinsame Nutzung mit Lese- und Schreibzugriff oder Schreibschutz für alle Clients freigegeben.

rw=*accesslist*
: Die Festlegung der gemeinsamen Nutzung des Dateisystems mit Lese- und Schreibzugriff wird nur für gelistete Clients durchgeführt. Alle anderen Anforderungen werden abgelehnt. Ab Solaris 2.6 wurde die Liste der Clients erweitert, die in *accesslist* definiert sind. Weitere Informationen finden Sie unter „Einrichten von Zugriffslisten mit dem `share`-Befehl“ auf Seite 175. Sie können diese Option verwenden, um eine `-ro`-Option außer Kraft zu setzen.

NFS-spezifische `share`-Optionen

Folgende Optionen können Sie für NFS-Dateisysteme verwenden.

aclok
: Mithilfe dieser Option kann ein NFS-Server, der das Protokoll der NFS-Version 2 unterstützt, so konfiguriert werden, dass er den Zugriff für Clients der NFS-Version 2 steuert. Ohne Angabe dieser Option erhalten alle Clients minimalen Zugriff. Bei Angabe dieser Option erhalten die Clients maximalen Zugriff. Wenn beispielsweise auf Dateisystemen, die mit der Option `-aclok` zur gemeinsamen Nutzung freigegeben werden, ein Benutzer über Leseberechtigungen verfügt, verfügen alle Benutzer über Leseberechtigungen. Ohne Angabe dieser Option können Sie jedoch einem Client, der normalerweise über Zugriffsberechtigungen verfügen sollte, den Zugriff verweigern. Eine Entscheidung über die Gewährung von Zugriffsberechtigungen hängt davon ab, welche Sicherheitssysteme bereits aktiv sind. Weitere Informationen zu Zugriffskontrolllisten (ACLs) finden Sie unter „Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Hinweis – Um Zugriffskontrolllisten zu verwenden, stellen Sie sicher, dass auf den betreffenden Clients und Servern eine Software ausgeführt wird, die NFS-Version 3 und die NFS_ACL-Protokolle unterstützt. Wenn die Software nur das Protokoll der NFS-Version 3 unterstützt, erhalten die Clients Zugriff, können aber nicht die Zugriffskontrolllisten manipulieren. Wenn die Software das NFS_ACL-Protokoll unterstützt, erhalten die Clients Zugriff und können die Zugriffskontrolllisten manipulieren.

anon=*uid*
: Mithilfe von *uid* wählen Sie die Benutzer-ID von nicht authentifizierten Benutzern. Wenn Sie *uid* auf `-1` setzen, verweigert der Server nicht authentifizierten Benutzern den Zugriff. Sie können den Root-Zugriff gewähren, indem Sie `anon=0` festlegen. Da diese Option bewirkt, dass nicht authentifizierten Benutzern Root-Zugriff gewährt wird, sollten Sie stattdessen die Option `root` verwenden.

index=*filename*
: Wenn ein Benutzer auf eine NFS-URL zugreift, erzwingt die `-index=`*filename*-Option das Laden der HTML-Datei, anstatt eine Liste des Verzeichnisses anzuzeigen. Mit dieser Option wird das Verhalten von gängigen Browsern imitiert, wenn eine `index.html`-Datei in dem Verzeichnis gefunden wird, auf das über die HTTP-URL zugegriffen wird. Die Verwendung dieser Option entspricht der Verwendung der `DirectoryIndex`-Option für `httpd`. Der `dfstab`-Dateieintrag sieht beispielsweise wie folgt aus:

```
share -F nfs -o ro,public,index=index.html /export/web
```

Diese URLs zeigen dann dieselben Informationen an:

```
nfs://<server>/<dir>
nfs://<server>/<dir>/index.html
nfs://<server>//export/web/<dir>
nfs://<server>//export/web/<dir>/index.html
http://<server>/<dir>
http://<server>/<dir>/index.html
```

log=*tag*
: Mit dieser Option wird das Tag in `/etc/nfs/nfslog.conf` angegeben, das die Konfigurationsinformationen der NFS-Serverprotokollierung für ein Dateisystem enthält. Diese Option muss angegeben werden, um die NFS-Serverprotokollierung zu aktivieren.

nosuid
: Mit dieser Option wird signalisiert, dass alle Versuche, den `setuid`-Modus oder den `setgid`-Modus zu aktivieren, ignoriert werden sollen. NFS-Clients können keine Dateien erstellen, wenn das Bit `setuid` oder das Bit `setgid` gesetzt ist.

public
: Die Option `-public` wurde dem Befehl `share` hinzugefügt, um WebNFS-Suchvorgänge zu ermöglichen. Mit dieser Option kann nur ein Dateisystem auf einem Server zur gemeinsamen Nutzung freigegeben werden.

root=*accesslist*
: Der Server gewährt den in der Liste angegebenen Hosts Root-Zugriff. Der Server gewährt den Remote-Hosts standardmäßig keinen Root-Zugriff. Wenn `-sec=sys` nicht der gewählte Sicherheitsmodus ist, können Sie nur die Client-Hostnamen in die Zugriffsliste (*accesslist*) aufnehmen. Ab Solaris 2.6 wurde die Liste der Clients erweitert, die in *accesslist* definiert sind. Weitere Informationen finden Sie unter „Einrichten von Zugriffslisten mit dem `share`-Befehl“ auf Seite 175.

Achtung – Wenn anderen Hosts Root-Zugriff gewährt wird, hat dies weitreichende Konsequenzen für die Sicherheit. Verwenden Sie die `-root=`-Option mit äußerster Vorsicht.

root=*client-name*
: Der *client-name*-Wert wird in Verbindung mit der AUTH_SYS-Authentifizierung verwendet, um die IP-Adresse des Clients mit einer Liste von Adressen abzugleichen, die von `exportfs(1B)` bereitgestellt wird. Wenn eine Übereinstimmung gefunden wird, wird den gemeinsam genutzten Dateisystemen der Zugriff auf `root` gewährt.

root=*host-name*
: Bei sicheren NFS-Modi wie beispielsweise AUTH_SYS oder RPCSEC_GSS gleicht der Server die Hauptnamen des Clients mit einer Liste von hostbasierten Hauptnamen ab, die aus einer Zugriffsliste abgeleitet werden. Für den Hauptnamen des Clients wird die Syntax `root@`*hostname* verwendet. Für Kerberos V wird die Syntax `root/`*hostname.fully.qualified* `@REALM` verwendet. Wenn Sie den *host-name*-Wert verwenden, müssen die in der Zugriffsliste aufgeführten Clients über die Berechtigungsnachweise für einen Hauptnamen verfügen. Für Kerberos V muss der Client einen gültigen Schlüsseltabelleneintrag für seinen `root/` *hostname.fully.qualified*`@REALM`-Hauptnamen haben. Weitere Informationen finden Sie unter „Konfigurieren von Kerberos-Clients“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

sec=*mode*[:*mode*]
: Mit *mode* werden die Sicherheitsmodi ausgewählt, die benötigt werden, um einen Zugriff auf das Dateisystem zu erhalten. Der standardmäßige Sicherheitsmodus ist die UNIX-Authentifizierung. Sie können mehrere Modi angeben, aber jeden Sicherheitsmodus nur einmal pro Befehlszeile verwenden. Jede `-mode`-Option gilt für alle nachfolgenden `-rw`-, `-ro`-, `-rw=`-, `-ro=`-, `-root=`- und `-window=`-Optionen, bis ein anderer `-mode` vorgefunden wird. Durch die Verwendung von `-sec=none` werden alle Benutzer dem Benutzer `nobody` zugeordnet.

window=*value*
: Mit *value* wird die maximale Lebensdauer in Sekunden festgelegt, die für einen Berechtigungsnachweis auf dem NFS-Server gilt. Der Standardwert beträgt 30000 Sekunden oder 8,3 Stunden.

Einrichten von Zugriffslisten mit dem `share`-Befehl

In Solaris-Versionen vor Version 2.6 war *accesslist*die in der `-ro=`-, `-rw=`- oder `-root=`-Option des `share`-Befehls enthaltene Zugriffsliste auf Hostnamen oder Netzgruppennamen beschränkt. Ab Solaris 2.6 kann die Zugriffsliste auch einen Domainnamen, eine Teilnetznummer oder einen Eintrag zur Zugriffsverweigerung enthalten. Diese Erweiterungen haben den Zweck, die Dateizugriffssteuerung auf einem einzelnen Server zu vereinfachen, ohne den Namespace ändern oder lange Listen von Clients verwalten zu müssen.

Mit diesem Befehl wird der Zugriff mit Schreibschutz für die meisten Systeme gewährt. Für `rose` und `lilac` jedoch wird der Lese- und Schreibzugriff gewährt:

```
# share -F nfs -o ro,rw=rose:lilac /usr/src
```

Im nächsten Beispiel wird jedem Host in der `eng`-Netzgruppe Zugriff mit Schreibschutz gewährt. Dem Client `rose` wird Lese- und Schreibzugriff gewährt.

```
# share -F nfs -o ro=eng,rw=rose /usr/src
```

Hinweis – Sie können weder `rw` noch `ro` ohne Argumente angeben. Wenn keine Lese- und Schreibzugriffsoption angegeben wird, ist der Lese- und Schreibzugriff standardmäßig für alle Clients aktiviert.

Um ein Dateisystem mit mehreren Clients freizugeben, müssen Sie alle Optionen auf der gleichen Zeile angeben. Bei mehreren Aufrufen des `share`-Befehls für dasselbe Objekt "merkt" sich das System nur den zuletzt ausgeführten Befehl. Mit diesem Befehl wird der Lese- und Schreibzugriff für drei Clientsysteme aktiviert, aber es wird nur `rose` und `tulip` wird Zugriff auf das Dateisystem als `root` gewährt.

```
# share -F nfs -o rw=rose:lilac:tulip,root=rose:tulip /usr/src
```

Wenn ein Dateisystem gemeinsam genutzt wird, das mehrere Authentifizierungsmechanismen verwendet, müssen Sie die Optionen `-ro`, `-ro=`, `-rw`, `-rw=`, `-root` und `-window` hinter den korrekten Sicherheitsmodi einfügen. In diesem Beispiel ist die UNIX-Authentifizierung für alle Hosts in der Netzgruppe namens `eng` ausgewählt. Diese Hosts können das Dateisystem nur im Schreibschutzmodus einhängen. Die Hosts `tulip` und `lilac` können das Dateisystem mit Lese- und Schreibzugriff einhängen, wenn sie die Diffie-Hellman-Authentifizierung verwenden. Mit diesen Optionen können `tulip` und `lilac` das Dateisystem auch dann mit Lese- und Schreibzugriff einhängen, wenn sie nicht die DH-Authentifizierung verwenden. Die Hostnamen müssen jedoch in der `eng`-Netzgruppe aufgelistet sein.

```
# share -F nfs -o sec=dh,rw=tulip:lilac,sec=sys,ro=eng /usr/src
```

Obwohl die UNIX-Authentifizierung der standardmäßige Sicherheitsmodus ist, wird die UNIX-Authentifizierung nicht einbezogen, wenn die Option `-sec` verwendet wird. Aus diesem

Grund müssen Sie eine `-sec=sys`-Option einfügen, wenn die UNIX-Authentifizierung zusammen mit anderen Authentifizierungsmechanismen verwendet werden soll.

Sie können einen DNS-Domainnamen in der Zugriffsliste verwenden, indem Sie einen Punkt vor den Domainnamen setzen. Die Zeichenfolge, die nach dem Punkt folgt, ist ein Domainname, aber kein voll qualifizierter Hostname. Durch den folgenden Eintrag wird allen Hosts in der `eng.example.com`-Domain Zugriff für das Einhängen gewährt:

```
# share -F nfs -o ro=.:.eng.example.com /export/share/man
```

In diesem Beispiel stimmt der Punkt (`.`) mit allen Hosts überein, die durch die NIS- oder NIS+-Namespaces abgeglichen werden. In den Ergebnissen, die von diesen Name Services zurückgegeben werden, ist der Domainname nicht enthalten. Der `.eng.example.com`-Eintrag stimmt mit allen Hosts überein, die für die Namespace-Auflösung DNS verwenden. DNS gibt immer einen voll qualifizierten Hostnamen zurück. Aus diesem Grund wird der längere Eintrag benötigt, wenn Sie eine Kombination aus DNS und anderen Namespaces verwenden.

Sie können eine Teilnetznummer in einer Zugriffsliste verwenden, indem Sie `@` vor die Netzwerknummer oder den Netzwerknamen setzen. Durch dieses Zeichen wird der Netzwerkname von einer Netzgruppe oder einem voll qualifizierten Hostnamen unterschieden. Sie müssen das Teilnetz in `/etc/networks` oder in einem NIS- oder NIS+-Namespace bestimmen. Die folgenden Einträge haben dieselbe Wirkung, wenn das `192.168`-Teilnetz als das `eng`-Netzwerk bestimmt wurde:

```
# share -F nfs -o ro=@eng /export/share/man
# share -F nfs -o ro=@192.168 /export/share/man
# share -F nfs -o ro=@192.168.0.0 /export/share/man
```

Die letzten beiden Einträge zeigen, dass Sie nicht die vollständige Netzwerkadresse angeben müssen.

Ist das Netzwerkpräfix nicht byteorientiert wie bei CIDR (Classless Inter-Domain Routing), kann die Maskenlänge explizit in der Befehlszeile angegeben werden. Die Maskenlänge wird definiert, indem hinter dem Netzwerknamen oder der Netzwerknummer ein Schrägstrich gesetzt wird und die signifikanten Bits im Präfix der Adresse angegeben werden. Beispiel:

```
# share -f nfs -o ro=@eng/17 /export/share/man
# share -F nfs -o ro=@192.168.0/17 /export/share/man
```

In diesen Beispielen bedeutet `/17`, dass die ersten 17 Bits in der Adresse als Maske verwendet werden sollen. Weitere Informationen zu CIDR können Sie RFC 1519 entnehmen.

Auch können Sie negativen Zugriff verwenden, indem Sie ein "`-`" vor den Eintrag setzen. Beachten Sie, dass die Einträge von links nach rechts gelesen werden. Darum müssen die negativen Zugriffseinträge vor dem Eintrag stehen, auf den sich die negativen Zugriffseinträge beziehen:

```
# share -F nfs -o ro=-rose:.eng.example.com /export/share/man
```

In diesem Beispiel wird allen Hosts in der `eng.example.com` -Domain Zugriff gewährt, abgesehen vom Host namens `rose`.

`unshare`-Befehl

Mit diesem Befehl wird die Verfügbarkeit eines Dateisystems aufgehoben, wodurch Clients keine Einhängungen mehr durchführen können. Sie können den Befehl `unshare` verwenden, um die gemeinsame Nutzung eines beliebigen Dateisystems aufzuheben, unabhängig davon, ob das Dateisystem explizit mit dem Befehl `share` oder automatisch durch `/etc/dfs/dfstab` zur gemeinsamen Nutzung freigegeben wurde. Wenn Sie den Befehl `unshare` verwenden, um die gemeinsame Nutzung eines Dateisystems aufzuheben, das Sie mithilfe der `dfstab`-Datei zur gemeinsamen Nutzung freigegeben haben, sollten Sie Vorsicht walten lassen. Beachten Sie, dass das Dateisystem wieder gemeinsam genutzt wird, wenn Sie den Vorgang beenden und wieder zur Betriebsebene 3 zurückkehren. Sie müssen den Eintrag für dieses Dateisystem aus der `dfstab`-Datei entfernen, wenn die Änderung wirksam bleiben soll.

Wenn Sie die gemeinsame Nutzung eines NFS-Dateisystems aufheben, wird der Zugriff über Clients mit vorhandenen Einhängungen unterbunden. Das Dateisystem kann immer noch auf dem Client eingehängt sein, aber auf die Dateien kann nicht zugegriffen werden.

Hinweis – Informationen zur Verhaltensweise der NFS-Version 4, wenn die gemeinsame Nutzung eines Dateisystems aufgehoben wird und das Dateisystem anschließend wieder hierfür freigegeben wird, finden Sie unter „Aufheben der gemeinsamen Nutzung und erneutes Freigeben zur gemeinsamen Nutzung eines Dateisystems in NFS-Version 4“ auf Seite 188.

Es folgt ein Beispiel für die Aufhebung der gemeinsamen Nutzung eines bestimmten Dateisystems:

```
# unshare /usr/src
```

`shareall`-Befehl

Mit diesem Befehl können mehrere Dateisysteme zur gemeinsamen Nutzung freigegeben werden. Wenn keine Optionen verwendet werden, werden mit dem Befehl alle Dateisysteme in `/etc/dfs/dfstab` gemeinsam genutzt. Sie können einen Dateinamen einfügen, um den Namen einer Datei anzugeben, die zum Auflisten von `share` -Befehlszeilen dient. Wenn Sie keinen Dateinamen einfügen, wird `/etc/dfs/dfstab` geprüft. Wenn Sie einen Bindestrich (`-`) verwenden, um den Dateinamen zu ersetzen, können Sie `share`-Befehle über die Standardeingabe eintragen.

Es folgt ein Beispiel für die Freigabe aller Dateisysteme zur gemeinsamen Nutzung, die in einer lokalen Datei aufgelistet sind:

```
# shareall /etc/dfs/special_dfstab
```

unshareall-Befehl

Mit diesem Befehl wird die Verfügbarkeit aller gemeinsam genutzten Ressourcen aufgehoben. Mit der `-F` *FSType*-Option wird eine Liste von Dateisystemtypen ausgewählt, die in `/etc/dfs/fstypes` definiert sind. Dieses Flag ermöglicht Ihnen, bestimmte Dateisystemtypen auszuwählen, deren gemeinsame Nutzung aufgehoben werden soll. Der standardmäßige Dateisystemtyp ist in `/etc/dfs/fstypes` definiert. Um bestimmte Dateisysteme auszuwählen, verwenden Sie den Befehl `unshare`.

Es folgt ein Beispiel für die Aufhebung der gemeinsamen Nutzung aller NFS-Dateisysteme:

```
# unshareall -F nfs
```

showmount-Befehl

Mit diesem Befehl wird Folgendes angezeigt:

- Alle Clients mit Dateisystemen, die per Remote-Zugriff eingehängt wurden und über einen NFS-Server gemeinsam genutzt werden
- Nur Dateisysteme, die von Clients eingehängt wurden
- Gemeinsam genutzte Dateisysteme mit Client-Zugriffsinformationen

---

Hinweis – Mit dem Befehl `showmount` werden nur die Exporte der NFS-Versionen 2 und 3 angezeigt. Mit dem Befehl werden keine Exporte der NFS-Version 4 angezeigt.

Es folgt die Befehlssyntax:

`showmount [ -ade ] [` *hostname* `]`

`-a`	Gibt eine Liste aller Remote-Einhängungen aus. In jedem Eintrag ist der Clientname und das Verzeichnis enthalten.
`-d`	Gibt eine Liste der Verzeichnisse aus, die von Clients per Remote-Zugriff eingehängt wurden.
`-e`	Gibt eine Liste der Dateien aus, die gemeinsam genutzt werden oder exportiert wurden.
hostname	Wählt den NFS-Server aus, der zum Sammeln der Informationen dient.

Wenn *hostname* nicht angegeben ist, wird der lokale Host abgefragt.

Mit dem folgenden Befehl werden alle Clients sowie die lokalen Verzeichnisse aufgelistet, die von den Clients eingehängt wurden:

```
# showmount -a bee
lilac:/export/share/man
lilac:/usr/src
rose:/usr/src
tulip:/export/share/man
```

Mit dem folgenden Befehl werden die Verzeichnisse aufgelistet, die eingehängt wurden:

```
# showmount -d bee
/export/share/man
/usr/src
```

Mit dem folgenden Befehl werden die Dateisysteme aufgelistet, die gemeinsam genutzt werden:

```
# showmount -e bee
/usr/src                              (everyone)
/export/share/man                   eng
```

`setmnt`-Befehl

Mit diesem Befehl wird eine `/etc/mnttab`-Tabelle erstellt. Mit den Befehlen `mount` und `umount` wird die Tabelle abgefragt. In der Regel müssen Sie diesen Befehl nicht manuell ausführen, da dieser Befehl automatisch ausgeführt wird, wenn das System neu gestartet wird.

Befehle zum Beheben von NFS-Problemen

Mit diesen Befehlen können NFS-Probleme behoben werden.

`nfsstat`-Befehl

Mit diesem Befehl können Sie statistische Informationen zu NFS- und RPC-Verbindungen sammeln. Die Syntax des Befehls lautet folgendermaßen:

`nfsstat [ -cmnrsz ]`

`-c` Zeigt clientseitige Informationen an.

`-m` Zeigt Statistiken für jedes mit NFS eingehängte Dateisystem an.

`-n` Gibt an, dass NFS-Informationen sowohl auf der Clientseite als auch auf der Serverseite angezeigt werden sollen.

`-r` Zeigt RPC-Statistiken an.

`-s` Zeigt serverseitige Informationen an.

`-z` Gibt an, dass die Statistiken auf null gesetzt werden sollen.

Wenn keine Optionen in der Befehlszeile angegeben werden, werden die `-cnrs`-Optionen verwendet.

Das Sammeln von serverseitigen Statistiken kann wichtig für die Behebung von Problemen sein, wenn neue Software oder neue Hardware in die Datenverarbeitungsumgebung integriert wird. Wenn dieser Befehl mindestens einmal pro Woche ausgeführt wird und die Ergebnisse gespeichert werden, können die erzielten Leistungen bestens nachverfolgt werden.

Siehe folgendes Beispiel:

```
# nfsstat -s

Server rpc:
Connection oriented:
calls      badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
719949194  0          0          0          0          58478624   33
Connectionless:
calls      badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
73753609   0          0          0          0          987278     7254

Server nfs:
calls                badcalls
787783794            3516
Version 2: (746607 calls)
null       getattr    setattr    root       lookup     readlink   read
883 0%     60 0%      45 0%      0 0%       177446 23% 1489 0%    537366 71%
wrcache    write      create     remove     rename     link       symlink
0 0%       1105 0%    47 0%      59 0%      28 0%      10 0%      9 0%
mkdir      rmdir      readdir    statfs
26 0%      0 0%       27926 3%   108 0%
Version 3: (728863853 calls)
null          getattr       setattr       lookup        access
1365467 0%    496667075 68% 8864191 1%    66510206 9%   19131659 2%
readlink      read          write         create        mkdir
414705 0%     80123469 10%  18740690 2%   4135195 0%    327059 0%
symlink       mknod         remove        rmdir         rename
101415 0%     9605 0%       6533288 0%    111810 0%     366267 0%
link          readdir       readdirplus   fsstat        fsinfo
2572965 0%    519346 0%     2726631 0%    13320640 1%   60161 0%
pathconf      commit
13181 0%      6248828 0%
Version 4: (54871870 calls)
null               compound
266963 0%          54604907 99%
Version 4: (167573814 operations)
reserved           access              close               commit
0 0%               2663957 1%          2692328 1%          1166001 0%
create             delegpurge          delegreturn         getattr
167423 0%          0 0%                1802019 1%          26405254 15%
```

```
getfh               link                lock                lockt
11534581 6%         113212 0%           207723 0%           265 0%
locku               lookup              lookupp             nverify
230430 0%           11059722 6%         423514 0%           21386866 12%
open                openattr            open_confirm        open_downgrade
2835459 1%          4138 0%             18959 0%            3106 0%
putfh               putpubfh            putrootfh           read
52606920 31%        0 0%                35776 0%            4325432 2%
readdir             readlink            remove              rename
606651 0%           38043 0%            560797 0%           248990 0%
renew               restorefh           savefh              secinfo
2330092 1%          8711358 5%          11639329 6%         19384 0%
setattr             setclientid         setclientid_confirm verify
453126 0%           16349 0%            16356 0%            2484 0%
write               release_lockowner   illegal
3247770 1%          0 0%                0 0%

Server nfs_acl:
Version 2: (694979 calls)
null        getacl      setacl      getattr     access      getxattrdir
0 0%        42358 6%    0 0%        584553 84%  68068 9%    0 0%
Version 3: (2465011 calls)
null        getacl      setacl      getxattrdir
0 0%        1293312 52% 1131 0%     1170568 47%
```

Die oben dargestellte Auflistung ist ein Beispiel für NFS-Serverstatistiken. Die ersten fünf Zeilen beziehen sich auf RPC und die übrigen Zeilen auf die Meldung von NFS-Vorgängen. Beide Statistiken geben Aufschluss über die durchschnittliche Anzahl von `badcalls` oder `calls` pro Woche. Dies kann bei der Erkennung eines Problems hilfreich sein. Der `badcalls`-Wert dient zur Angabe der Anzahl von ungültigen Meldungen, die ein Client gesendet hat. Dieser Wert kann auf Probleme mit der Netzwerkhardware hindeuten.

Aus manchen Verbindungen resultieren Schreibvorgänge auf den Datenträgern. Ein plötzlicher Anstieg in diesen Statistiken kann auf ein Problem hindeuten. Dann sollte eine Untersuchung durchgeführt werden. Bei Statistiken der NFS-Version 2 sollte auf die Verbindungen `setattr`, `write`, `create`, `remove`, `rename` , `link`, `symlink`, `mkdir` und `rmdir` geachtet werden. Bei Statistiken der NFS-Versionen 3 und 4 sollte auf den Wert `commit` geachtet werden. Wenn der Wert von `commit` bei einem NFS-Server im Vergleich mit einem anderen, fast identischen Server relativ hoch ist, prüfen Sie, ob die NFS-Clients über genügend Speicher verfügen. Die Anzahl der `commit`-Vorgänge auf dem Server steigt an, wenn Clients keine verfügbaren Ressourcen haben.

`pstack`-Befehl

Mit diesem Befehl wird ein Datenstapelprotokoll für jeden Prozess angezeigt. Der Befehl `pstack` muss vom Eigentümer des Prozesses oder vom `root`-Benutzer ausgeführt werden. Sie können `pstack` verwenden, um festzustellen, wo ein Prozess hängt. Die einzige Option, die in Verbindung mit diesem Befehl verwendet werden darf, ist die `PID`-Option des Prozesses, der von Ihnen überprüft werden muss. Weitere Informationen finden Sie auf der Manpage `proc(1)`.

Im folgenden Beispiel wird der laufende `nfsd`-Prozess geprüft.

```
# /usr/bin/pgrep nfsd
243
# /usr/bin/pstack 243
243:    /usr/lib/nfs/nfsd -a 16
 ef675c04 poll     (24d50, 2, ffffffff)
 000115dc ???????? (24000, 132c4, 276d8, 1329c, 276d8, 0)
 00011390 main     (3, effff14, 0, 0, ffffffff, 400) + 3c8
 00010fb0 _start   (0, 0, 0, 0, 0, 0) + 5c
```

Das Beispiel zeigt, dass der Prozess auf eine neue Verbindungsanforderung wartet, was eine normale Antwort ist. Wenn der Stapel zeigt, dass der Prozess nach der Absendung einer Anforderung weiterhin abgefragt wird, hängt der Prozess möglicherweise. Führen Sie die unter „So starten Sie die NFS-Services neu“ auf Seite 130 beschriebenen Schritte aus, um das Problem zu beheben. Gehen Sie nochmals die unter „NFS-Fehlerbehebungsverfahren“ auf Seite 125 beschriebenen Schritte durch, um sicherzugehen, dass das Problem auf einen hängenden Prozess oder ein hängendes Programm zurückzuführen ist.

`rpcinfo`-Befehl

Mit diesem Befehl werden Informationen zum RPC-Service generiert, der auf einem System ausgeführt wird. Sie können mit diesem Befehl auch den RPC-Service ändern. Für diesen Befehl stehen zahlreiche Optionen zur Verfügung. Weitere Informationen finden Sie auf der Manpage `rpcinfo(1M)`. Es folgt eine kurze Darstellung von einigen der Optionen, die Sie in Verbindung mit diesem Befehl verwenden können:

`rpcinfo [ -m | -s ] [` *hostname* `]`

`rpcinfo -T` *transport hostname* `[` *progname* `]`

`rpcinfo [ -t | -u ] [` *hostname* `] [` *progname* `]`

`-m`	Zeigt eine Tabelle mit Statistiken der `rpcbind`-Vorgänge an.
`-s`	Zeigt eine kurze Liste aller registrierten RPC-Programme an.
`-T`	Zeigt Informationen zu Services an, die spezielle Übertragungsverfahren oder Protokolle verwenden.
`-t`	Untersucht die RPC-Programme, die TCP verwenden.
`-u`	Untersucht die RPC-Programme, die UDP verwenden.
transport	Wählt das Übertragungsverfahren oder Protokoll für die Services aus.
hostname	Wählt den Hostnamen des Servers aus, von dem Sie Informationen benötigen.

progname Wählt das RPC-Programm aus, über das Informationen gesammelt werden sollen.

Wenn kein Wert für *hostname* angegeben ist, wird der lokale Hostname verwendet. Sie können *progname* durch eine RPC-Programmnummer ersetzen. Bedenken Sie aber, dass sich viele Benutzer an den Namen erinnern können, nicht aber an die Nummer. Bei Systemen, auf denen die Software der NFS-Version 3 nicht ausgeführt wird, können Sie die Option `-p` anstelle der Option `-s` verwenden.

Die Daten, die durch diesen Befehl bereitgestellt werden, können Folgendes enthalten:

- Die RPC-Programmnummer
- Die Versionsnummer für ein bestimmtes Programm
- Das verwendete Transportprotokoll
- Den Namen des RPC-Service
- Den Eigentümer des RPC-Service

Im folgenden Beispiel werden Informationen zu den RPC-Services gesammelt, die auf einem Server ausgeführt werden. Der Text, der durch die Ausführung des Befehls erstellt wurde, wird mithilfe des Befehls `sort` gefiltert, wodurch die Ausgabe lesbarer wird. Mehrere Zeilen, auf denen RPC-Services aufgelistet waren, wurden aus dem Beispiel entfernt.

```
% rpcinfo -s bee |sort -n
   program version(s) netid(s)                         service     owner
    100000  2,3,4     udp6,tcp6,udp,tcp,ticlts,ticotsord,ticots rpcbind     superuser
    100001  4,3,2     ticlts,udp,udp6                   rstatd      superuser
    100002  3,2       ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 rusersd     superuser
    100003  3,2       tcp,udp,tcp6,udp6                 nfs         superuser
    100005  3,2,1     ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 mountd      superuser
    100007  1,2,3     ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 ypbind      superuser
    100008  1         ticlts,udp,udp6                   walld       superuser
    100011  1         ticlts,udp,udp6                   rquotad     superuser
    100012  1         ticlts,udp,udp6                   sprayd      superuser
    100021  4,3,2,1   tcp,udp,tcp6,udp6                 nlockmgr    superuser
    100024  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 status      superuser
    100029  3,2,1     ticots,ticotsord,ticlts           keyserv     superuser
    100068  5         tcp,udp                           cmsd        superuser
    100083  1         tcp,tcp6                          ttdbserverd superuser
    100099  3         ticotsord                         autofs      superuser
    100133  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    100134  1         ticotsord                         tokenring   superuser
    100155  1         ticots,ticotsord,tcp,tcp6         smserverd   superuser
    100221  1         tcp,tcp6                          -           superuser
    100227  3,2       tcp,udp,tcp6,udp6                 nfs_acl     superuser
    100229  1         tcp,tcp6                          metad       superuser
    100230  1         tcp,tcp6                          metamhd     superuser
    100231  1         ticots,ticotsord,ticlts           -           superuser
    100234  1         ticotsord                         gssd        superuser
    100235  1         tcp,tcp6                          -           superuser
    100242  1         tcp,tcp6                          metamedd    superuser
    100249  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    300326  4         tcp,tcp6                          -           superuser
```

```
    300598  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    390113  1         tcp                                       -           unknown
 805306368  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
1289637086  1,5       tcp                                       -           26069
```

Die folgenden zwei Beispiele zeigen, wie Informationen über einen bestimmten RPC-Service gesammelt werden, indem ein bestimmtes Übertragungsverfahren auf einem Server ausgewählt wird. Im ersten Beispiel wird der `mountd`-Service überprüft, der über TCP ausgeführt wird. Im zweiten Beispiel wird der NFS-Service überprüft, der über UDP ausgeführt wird.

```
% rpcinfo -t bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
% rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

snoop-Befehl

Dieser Befehl wird oft verwendet, um zu prüfen, ob im Netzwerk Pakete vorhanden sind. Der Befehl `snoop` muss als `root` ausgeführt werden. Mit dem Befehl kann sichergestellt werden, dass die Netzwerkhardware sowohl auf dem Client als auch auf dem Server funktioniert. Zahlreiche Optionen stehen zur Verfügung. Weitere Informationen finden Sie auf der Manpage `snoop(1M)`. Es folgt eine kurze Darstellung des Befehls:

`snoop [ -d` *device* `] [ -o` *filename* `] [ host` *hostname* `]`

`-d` *device*	Gibt die lokale Netzwerkschnittstelle an.
`-o` *filename*	Speichert alle erfassten Pakete im Dateinamen.
hostname	Zeigt nur Pakete an, die an einen bestimmten Host und von diesem gesendet werden.

Die Option `-d` *device* ist auf Servern hilfreich, die mehrere Netzwerkschnittstellen haben. Sie können viele Ausdrücke verwenden, anstatt den Host zu definieren. Durch eine Kombination von Befehlsaudrücken mit `grep` können Daten generiert werden, die spezifisch genug für eine nützliche Verwendung sind.

Stellen Sie bei der Fehlerbehebung sicher, dass Pakete an den richtigen Host und von diesem gesendet werden. Achten Sie auch auf Fehlermeldungen. Durch das Speichern der Pakete in einer Datei kann das Prüfen der Daten vereinfacht werden.

`truss`-Befehl

Sie können diesen Befehl zum Prüfen verwenden, wenn ein Prozess hängt. Der Befehl `truss` muss vom Eigentümer des Prozesses oder vom `root`-Benutzer ausgeführt werden. Sie können viele Optionen in Verbindung mit diesem Befehl verwenden. Weitere Informationen finden Sie auf der Manpage `truss(1)`. Es folgt eine kurze Syntax des Befehls:

`truss [ -t` *syscall* `] -p` *pid*

`-t` *syscall* Wählt Systemaufrufe aus, die verfolgt werden sollen.

`-p` *pid* Zeigt die PID des Prozesses an, der verfolgt werden soll.

syscall kann eine durch Komma getrennte Liste von Systemaufrufen sein, die verfolgt werden sollen. Wenn *syscall* mit `!` gestartet wird, werden die aufgelisteten Systemaufrufe aus der Ablaufverfolgung ausgeschlossen.

Das Beispiel zeigt, dass der Prozess erst dann fortgesetzt wird, wenn eine Verbindungsanforderung von einem neuen Client eingeht.

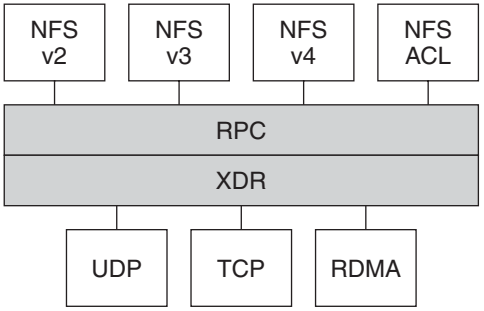
```
# /usr/bin/truss -p 243
poll(0x00024D50, 2, -1)         (sleeping...)
```

Im vorangegangenen Beispiel wird eine normale Antwort erzielt. Wenn sich die Antwort nicht ändert, nachdem eine neue Verbindungsanforderung gesendet wurde, hängt der Prozess möglicherweise. Führen Sie die unter „So starten Sie die NFS-Services neu“ auf Seite 130 beschriebenen Schritte aus, um das hängende Programm wiederherzustellen. Gehen Sie nochmals die unter „NFS-Fehlerbehebungsverfahren“ auf Seite 125 beschriebenen Schritte durch, um sicherzugehen, dass das Problem auf einen hängenden Prozess oder ein hängendes Programm zurückzuführen ist.

NFS über RDMA

Solaris 10 enthält ein RDMA-Protokoll (Remote Direct Memory Access). Hierbei handelt es sich um eine Technologie für die Übertragung von Daten zwischen Speichern über Hochgeschwindigkeitsnetzwerke. RDMA sorgt vor allem für die direkte Remote-Datenübertragung zwischen Speichern ohne Eingreifen der CPU. RDMA sorgt zudem für eine direkte Datenumsetzung, wodurch keine Datenkopien mehr benötigt werden und damit auch kein Eingreifen der CPU mehr erforderlich ist. Auf diese Weise entlastet RDMA nicht nur die Host-CPU, sondern reduziert auch Konflikte, die den Hostspeicher und E/A-Busse betreffen. Dies ist möglich, weil RDMA die E/A-Verbindungstechnologie der InfiniBand-on-SPARC-Plattformen mit den Funktionen des Betriebssystems Solaris vereint. Die folgende Abbildung zeigt die Beziehung zwischen RDMA und anderen Protokollen wie UDP und TCP.

ABBILDUNG 6–1 Beziehung von RDMA zu anderen Protokollen



NFS ist eine Protokollfamilie, die über RPC gelegen ist. Die XDR-(eXternal Data Representation-)Schicht kodiert RPC-Argumente und RPC-Ergebnisse auf einem der RPC-Übermittlungssysteme wie UDP, TCP und RDMA.

Wenn die RDMA-Übertragung weder auf dem Client noch auf dem Server verfügbar ist, wird zunächst auf die TCP-Übertragung zurückgegriffen und dann auf UDP, wenn TCP nicht verfügbar ist. Wenn Sie jedoch die `proto=rdma`-Einhängeoption verwenden, wird erzwungen, dass für NFS-Einhängungen ausschließlich RDMA verwendet wird.

Weitere Informationen zu NFS-Einhängeoptionen finden Sie auf der Manpage `mount_nfs(1M)` und unter „`mount`-Befehl“ auf Seite 162.

Hinweis – RDMA für InfiniBand verwendet das IP-Adressierungsformat und die IP-Suchstruktur, um Peers anzugeben. Da RDMA jedoch ein separater Protokollstapel ist, werden nicht alle IP-Semantikelemente vollständig implementiert. RDMA verwendet beispielsweise keine IP-Adressierung, um mit Peers zu kommunizieren. Darum können Konfigurationen aufgrund von verschiedenen, auf IP-Adressen basierenden Sicherheitsrichtlinien von RDMA umgangen werden. Jedoch werden die für NFS und RPC geltenden administrativen Richtlinien, beispielsweise `mount`-Beschränkungen und RPC-Sicherheit, nicht umgangen.

Funktionsweise des NFS-Service

In den folgenden Abschnitten werden einige der komplexen Funktionen der NFS-Software beschrieben. Beachten Sie, dass einige der in diesem Abschnitt enthaltenen Beschreibungen ausschließlich für die NFS-Version 4 gelten.

- „Versionsaushandlung in NFS“ auf Seite 187
- „Funktionen in NFS-Version 4“ auf Seite 188
- „UDP- und TCP-Aushandlung“ auf Seite 199
- „Aushandlung der Dateiübertragungsgröße“ auf Seite 200
- „Einhängen von Dateisystemen“ auf Seite 201
- „Funktionsweise der Option `-public` und der NFS-URLs beim Einhängen“ auf Seite 202
- „Clientseitiges Failover“ auf Seite 202
- „Große Dateien“ auf Seite 205
- „Funktionsweise der NFS-Serverprotokollierung“ auf Seite 205
- „Funktionsweise des WebNFS-Service“ auf Seite 206
- „WebNFS-Beschränkungen bei Verwendung eines Webbrowsers“ auf Seite 208
- „Sicheres NFS-System“ auf Seite 208
- „Secure RPC“ auf Seite 209

Hinweis – Wenn auf Ihrem System aktivierte Zonen vorhanden sind und Sie beabsichtigen, diese Funktion in einer nicht globalen Zone zu verwenden, lesen Sie *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*, um weitere Informationen zu erhalten.

Versionsaushandlung in NFS

Der NFS-Initiierungsprozess schließt die Aushandlung der Protokollebenen für Server und Clients ein. Wenn Sie keinen Versionsstand angeben, wird ein geeigneter Versionstand standardmäßig ausgewählt. Wenn beispielsweise sowohl der Server als auch der Client die Version 3 unterstützen, wird Version 3 verwendet. Wenn der Client oder der Server nur die Version 2 unterstützen, wird Version 2 verwendet.

Ab Solaris 10 können Sie die Schlüsselwörter NFS_CLIENT_VERSMIN, NFS_CLIENT_VERSMAX, NFS_SERVER_VERSMIN und NFS_SERVER_VERSMAX in der `/etc/default/nfs`-Datei angeben. Die von Ihnen angegebenen minimalen und maximalen Werte für den Server und den Client ersetzen die Standardwerte dieser Schlüsselwörter. Der minimale Standardwert für sowohl den Client als auch den Server ist 2, und der maximale Standardwert ist 4. Lesen Sie dazu „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144. Um festzustellen, welche Version vom Server unterstützt wird, beginnt der NFS-Client mit den Einstellungen für NFS_CLIENT_VERSMAX und fährt dann mit den weiteren Versionen fort, bis er die Versionseinstellung für NFS_CLIENT_VERSMIN erreicht. Sobald die unterstützte Version gefunden ist, wird der Vorgang beendet. Wenn beispielsweise NFS_CLIENT_VERSMAX=4 und NFS_CLIENT_VERSMIN=2 angegebenen sind, prüft der Client zunächst Version 4, dann Version 3 und zuletzt Version 2. Wenn NFS_CLIENT_VERSMIN und NFS_CLIENT_VERSMAX auf den gleichen Wert gesetzt sind, verwendet der Client stets die betreffende Version und versucht nicht, eine andere Version zu verwenden. Wenn der Server nicht über diese Version verfügt, schlägt die Einhängung fehl.

Hinweis – Sie können die durch die Aushandlung festgelegten Werte außer Kraft setzen, indem Sie die Option `vers` in Verbindung mit dem Befehl `mount` verwenden. Weitere Informationen finden Sie auf der Manpage `mount_nfs`(1M).

Informationen zur Verfahrensweise finden Sie unter „Einrichten von NFS-Services“ auf Seite 96.

Funktionen in NFS-Version 4

An NFS-Version 4 wurden viele Änderungen vorgenommen. In diesem Abschnitt werden diese neuen Funktionen beschrieben.

- „Aufheben der gemeinsamen Nutzung und erneutes Freigeben zur gemeinsamen Nutzung eines Dateisystems in NFS-Version 4“ auf Seite 188
- „Dateisystem-Namespace in NFS-Version 4“ auf Seite 189
- „Temporäre Dateizugriffsroutinen in NFS-Version 4“ auf Seite 191
- „Clientwiederherstellung in NFS-Version 4“ auf Seite 192
- „`OPEN`-Unterstützung zur gemeinsamen Nutzung in NFS-Version 4“ auf Seite 195
- „Delegierung in NFS-Version 4“ auf Seite 195
- „Zugriffskontrolllisten (ACLs) und `nfsmapid` in NFS-Version 4“ auf Seite 197
- „Clientseitiges Failover in NFS-Version 4“ auf Seite 204

Hinweis – Ab Solaris 10 unterstützt NFS-Version 4 nicht die LIPKEY/SPKM-Sicherheitsvariante. Außerdem werden die Dämonen `mountd` , `nfslogd` und `statd` nicht von NFS-Version 4 verwendet.

Verfahrensbezogene Informationen zur Verwendung der NFS-Version 4 finden Sie unter „Einrichten von NFS-Services“ auf Seite 96.

Aufheben der gemeinsamen Nutzung und erneutes Freigeben zur gemeinsamen Nutzung eines Dateisystems in NFS-Version 4

Wenn ein Client versucht, auf eine Dateisystem zuzugreifen, für den die gemeinsame Nutzung aufgehoben wurde, antwortet der Server sowohl bei Verwendung von NFS-Version 3 als auch NFS-Version 4 mit einem Fehlercode. In NFS-Version 3 werden von Clients veranlasste Sperre jedoch vom Server beibehalten, bevor die gemeinsame Nutzung des Dateisystems aufgehoben wird. Dadurch ist es nach der erneuten Freigabe zur gemeinsamen Nutzung des Dateisystems möglich, dass Clients der NFS-Version 3 auf das Dateisystem zugreifen, obwohl die gemeinsame Nutzung des Dateisystems nicht aufgehoben wurde.

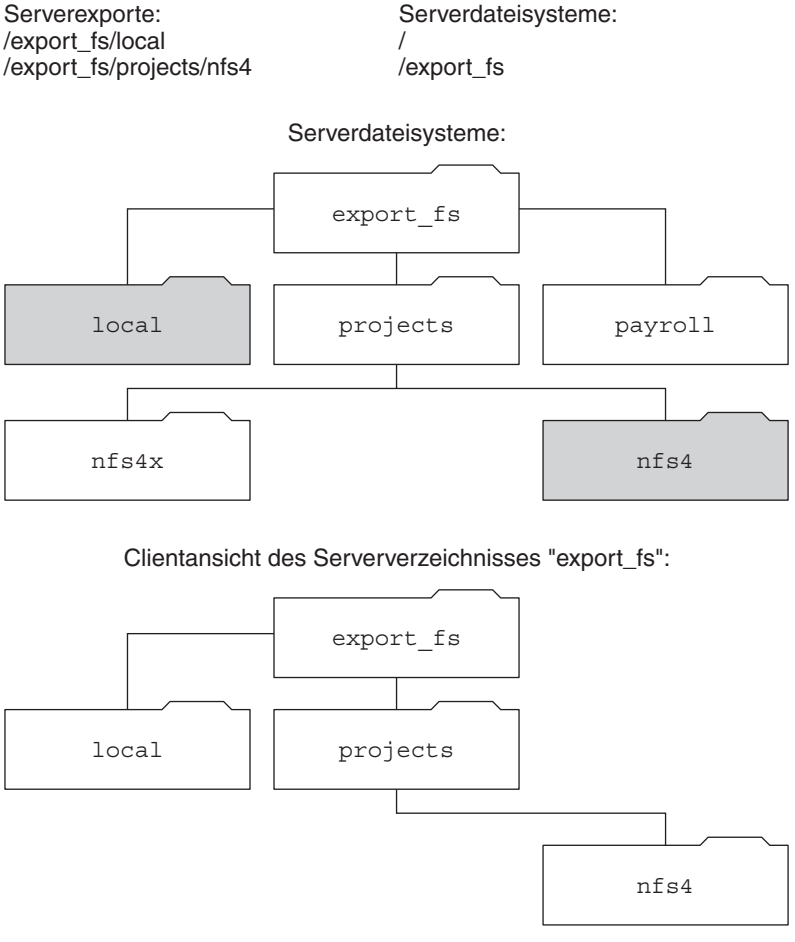
Wenn mit NFS-Version 4 die gemeinsame Nutzung eines Dateisystems aufgehoben wird, werden sämtliche Zustände von geöffneten Dateien oder Dateisperrungen im betreffenden Dateisystem außer Kraft gesetzt. Wenn der Client versucht, auf diese Dateien oder Sperren zuzugreifen, erhält er eine Fehlermeldung. Dieser Fehler wird der Anwendung normalerweise als `E/A`-Fehler gemeldet. Beachten Sie jedoch, dass durch die erneute Freigabe eines gemeinsam genutzten Dateisystems zum Zweck der Änderung von Optionen keine Zustände auf dem Server außer Kraft gesetzt werden.

Relevante Informationen finden Sie unter „Clientwiederherstellung in NFS-Version 4“ auf Seite 192 oder auf der Manpage `unshare_nfs(1M)`.

Dateisystem-Namespace in NFS-Version 4

Die Server der NFS-Version 4 erstellen und verwalten ein Pseudodateisystem, das Clients den mühelosen Zugriff auf alle exportierten Objekte auf einem Server ermöglicht. In den Vorgängerversionen war das Pseudodateisystem nicht vorhanden. Die Clients waren gezwungen, jedes gemeinsamgenutzte Serverdateisystem einzuhängen, um den Zugriff zu ermöglichen. Betrachten Sie das folgende Beispiel.

ABBILDUNG 6–2 Ansichten des Serverdateisystems und des Clientdateisystems



Beachten Sie, dass die Verzeichnisse `payroll` und `nfs4x` für den Client nicht sichtbar sind, da sie nicht exportiert wurden und nicht zu exportierten Verzeichnisse führen. Das Verzeichnis `local` ist jedoch für den Client sichtbar, da es sich um ein exportiertes Verzeichnis handelt. Das Verzeichnis `projects` ist für den Client sichtbar, da `projects` zum exportierten Verzeichnis `nfs4` führt. Dadurch werden nicht explizit exportierte Teile des Server-Namespace mit einem Pseudodateisystem überbrückt, das nur exportierte Verzeichnisse und Verzeichnisse anzeigt, die zu Serverexporten führen.

Ein Pseudodateisystem ist eine Struktur, die nur Verzeichnisse enthält und vom Server erstellt wird. Das Pseudodateisystem erlaubt einem Client, die Hierarchie von exportierten

Dateisystemen zu durchsuchen. Dadurch wird die Sicht des Clients auf das Pseudodateisystem durch die Pfade beschränkt, die zu den exportierten Dateisystemen führen.

Frühere Versionen von NFS ließen es nicht zu, dass Clients Serverdateisysteme durchqueren, ohne jedes Dateisystem einzuhängen. In NFS-Version 4 bewirkt der Server-Namespace jedoch Folgendes:

- Beschränkung der Dateisystemansicht des Clients auf Verzeichnisse, die zu Serverexporten führen
- Müheloser Zugriff auf Serverexporte für Clients, ohne dass die Clients die jeweils zugrunde liegenden Dateisysteme einhängen müssen Siehe vorangegangenes Beispiel. Beachten Sie jedoch, dass es aufgrund unterschiedlicher Betriebssysteme erforderlich sein kann, dass jedes Serverdateisystem vom Client eingehängt werden muss.

Aus POSIX-bezogenen Gründen überschreitet der Client der NFS-Version 4 von Solaris keine Grenzen des Serverdateisystems. Wenn dies vom Client versucht wird, wird ein leeres Verzeichnis angezeigt. Um dieses Problem zu beheben, müssen Sie jedes der Dateisysteme des Servers einhängen.

Temporäre Dateizugriffsroutinen in NFS-Version 4

Dateizugriffsroutinen werden auf dem Server erstellt und enthalten Informationen, mit deren Hilfe Dateien und Verzeichnisse eindeutig bestimmt werden können. In den NFS-Versionen 2 und 3 wurden vom Server dauerhafte Dateizugriffsroutinen zurückgegeben. Dadurch konnte der Client gewährleisten, dass der Server eine Dateizugriffsroutine generiert, die immer auf dieselbe Datei verweist. Beispiel:

- Wurde eine Datei gelöscht und durch eine Datei mit dem gleichen Namen ersetzt, generierte der Server eine neue Dateizugriffsroutine für die neue Datei. Wenn der Client eine alte Dateizugriffsroutine verwendete, gab der Server eine Fehlermeldung zurück, die darauf hinwies, dass die Dateizugriffsroutine veraltet war.
- Wenn eine Datei umbenannt wurde, blieb die Dateizugriffsroutine unverändert.
- Wenn Sie den Server neu starten mussten, sind die Dateizugriffsroutinen unverändert geblieben.

Wenn der Server eine auf eine Dateizugriffsroutine bezogene Anforderung von einem Client erhielt, konnte die Anforderung problemlos aufgelöst werden, wodurch die Dateizugriffsroutine immer auf die richtige Datei verwies.

Diese Methode zur Bestimmung von Dateien und Verzeichnissen für NFS-Vorgänge war für die meisten UNIX-basierten Server völlig ausreichend. Jedoch konnte die Methode nicht auf Servern implementiert werden, die andere Mittel zur Bestimmung verwendeten, beispielsweise den Pfadnamen einer Datei. Um dieses Problem zu lösen, gestattet das Protokoll der NFS-Version 4 einem Server, zu deklarieren, dass seine Dateizugriffsroutinen temporär sind.

Dadurch kann eine andere Dateizugriffsroutine verwendet werden. Ist dies der Fall, muss der Client nach der neuen Dateizugriffsroutine suchen.

Wie in den NFS-Versionen 2 und 3 von Solaris stellt auch der Server der NFS-Version 4 stets dauerhafte Dateizugriffsroutinen bereit. Jedoch müssen Clients der NFS-Version 4 von Solaris, die auf Server zugreifen, die keine Server der NFS-Version 4 von Solaris sind, temporäre Dateizugriffsroutinen unterstützen, wenn diese vom Server verwendet werden. Vor allem muss der Client die Zuordnung zwischen Pfadname und Dateizugriffsroutine zwischenspeichern, wenn ihm vom Server mitgeteilt wird, dass die Dateizugriffsroutine temporär ist. Der Client verwendet die temporäre Dateizugriffsroutine, bis ihre Nutzungsdauer abgelaufen ist. Sobald dies geschehen ist, führt der Client folgende Vorgänge aus:

- Entfernen der zwischengespeicherten Informationen, die sich auf die Dateizugriffsroutine beziehen
- Suchen nach der neuen Dateizugriffsroutine für die betreffende Datei
- Versuchen, den Vorgang zu wiederholen

Hinweis – Der Server teilt dem Client stets mit, welche Dateizugriffsroutinen dauerhaft und welche Dateizugriffsroutinen temporär sind.

Die Nutzungsdauer von temporären Dateizugriffsroutinen kann aus folgenden Gründen ablaufen:

- Eine Datei wird geschlossen.
- Das Dateisystem der Dateizugriffsroutine wird migriert.
- Ein Client benennt eine Datei um.
- Server wird neu gestartet.

Beachten Sie Folgendes: Wenn der Client die neue Dateizugriffsroutine nicht finden kann, wird eine Fehlermeldung in die `syslog`-Datei geschrieben. Weitere Versuche des Zugriffs auf diese Datei schlagen fehl, und es wird ein `E/A`-Fehler ausgegeben.

Clientwiederherstellung in NFS-Version 4

Das Protokoll der NFS-Version 4 ist ein statusbehaftetes Protokoll. Ein Protokoll ist statusbehaftet, wenn der Client und der Server aktuelle Informationen über Folgendes verwahren:

- Offene Dateien
- Dateisperren

Bei einem Ausfall wie beispielsweise einem Serverabsturz arbeiten der Client und der Server zusammen, um den Status vor dem Ausfall (offen und gesperrt) wiederherzustellen.

Wenn ein Server abstürzt und neu gestartet wird, geht der Status des Servers verloren. Der Client erkennt, dass der Server neu gestartet wurde und beginnt, den Server dabei zu unterstützen, seinen Status wiederherzustellen. Dieser Prozess wird als Clientwiederherstellung bezeichnet, da er vom Client gesteuert wird.

Wenn der Client feststellt, dass der Server neu gestartet wurde, stellt der Client sofort seine laufenden Aktivitäten ein und beginnt mit dem Prozess der Clientwiederherstellung. Wenn die Wiederherstellung beginnt, wird eine Meldung wie die folgende in das Systemfehlerprotokoll `/var/adm/messages` eingetragen:

```
NOTICE: Starting recovery server basil.example.company.com
```

Während der Wiederherstellung sendet der Client die Informationen, die Aufschluss über den vorherigen Status des Clients geben, an den Server. Beachten Sie jedoch, dass der Client in diesem Zeitraum keine neuen Anforderungen an den Server sendet. Neue Anforderungen für das Öffnen oder Sperren von Dateien können erst dann gesendet werden, wenn der Server die Wiederherstellung abgeschlossen hat.

Wenn die Clientwiederherstellung abgeschlossen ist, wird eine Meldung wie die folgende in das Systemfehlerprotokoll `/var/adm/messages` eingetragen:

```
NOTICE: Recovery done for server basil.example.company.com
```

Jetzt ist der Vorgang erfolgreich abgeschlossen (der Client hat seine Statusinformationen an den Server gesendet). Obwohl der Client diesen Vorgang abgeschlossen hat, kann es sein, dass dies bei anderen Clients noch nicht der Fall ist. Aus diesem Grund akzeptiert der Server über einen bestimmten Zeitraum keine Anforderungen für das Öffnen oder Sperren von Dateien. Diese Zeitspanne, die als Wartezeit bezeichnet wird, gestattet allen Clients, ihre Wiederherstellung abzuschließen.

Wenn der Client während dieser Wartezeit versucht, neue Dateien zu öffnen oder neue Sperren festzulegen, wird die betreffende Anforderung verweigert und der Fehlercode `GRACE` ausgegeben. Nach Empfang dieses Fehlers muss der Client warten, bis die Wartezeit abgelaufen ist. Sobald dies geschehen ist, kann der Client die Anforderung erneut an den Server senden. Während der Wartezeit wird die folgende Meldung angezeigt:

```
NFS server recovering
```

Während der Wartezeit kann die Ausführung von Befehlen fortgesetzt werden, die nicht das Öffnen oder Sperren von Dateien veranlassen. Dies sind beispielsweise die Befehle `ls` und `cd`. Die Ausführung dieser Befehle wird nicht ausgesetzt. Jedoch wird die Ausführung eines Befehls wie beispielsweise `cat`, der das Öffnen einer Datei veranlasst, bis zum Ende der Wartezeit ausgesetzt.

Sobald die Wartezeit abgelaufen ist, wird die folgende Meldung angezeigt:

```
NFS server recovery ok.
```

Der Client kann nun neue Anforderungen für das Öffnen und Sperren von Dateien an den Server senden.

Die Clientwiederherstellung kann aus verschiedenen Gründen fehlschlagen. Wenn beispielsweise nach dem Neustart des Servers eine Netzwerkpartition vorhanden ist, kann der Client seinen Status eventuell nicht mithilfe des Servers wiederherstellen, bevor die Wartezeit abgelaufen ist. Nach Ablauf der Wartezeit gestattet der Server dem Client nicht, seinen Status wiederherzustellen, da aus neuen statusbehafteten Vorgängen Konflikte resultieren können. Eine neue Dateisperre kann beispielsweise mit einer alten Dateisperre in Konflikt geraten, wenn der Client versucht, die alte Dateisperre wiederherzustellen. In einem solchen Fall gibt der Server den Fehlercode `NO_GRACE` an den Client zurück.

Wenn die Wiederherstellung eines Öffnungsvorgangs für eine bestimmte Datei fehlschlägt, kennzeichnet der Client die Dateien als nicht verwendbar, wodurch die folgende Meldung angezeigt wird.

```
WARNING: The following NFS file could not be recovered and was marked dead
(can't reopen:  NFS status 70):  file :  filename
```

Der Wert `70` dient nur als Beispiel.

Wenn die Wiederherstellung einer Dateisperre fehlschlägt, wird die folgende Fehlermeldung ausgegeben:

```
NOTICE: nfs4_send_siglost:  pid PROCESS-ID lost
lock on server SERVER-NAME
```

In solch einem Fall wird das auf den betreffenden Prozess bezogene Signal `SIGLOST` ausgegeben. Nach der Ausgabe des Signals `SIGLOST` wird der Prozess standardmäßig beendet.

Um diesen Status zu beseitigen, müssen Sie alle Anwendung neu starten, bei denen zum Zeitpunkt des Ausfalls Dateien geöffnet waren. Dann kann Folgendes auftreten:

- Manche Prozesse, die die betreffende Datei nicht erneut geöffnet haben, empfangen `E/A`-Fehler.
- Andere Prozesse, die die Datei erneut geöffnet haben oder nach der fehlgeschlagenen Wiederherstellung den Öffnungsvorgang ausgeführt haben, können ohne Probleme auf die Datei zugreifen.

Manche Prozesse können also auf eine bestimmte Datei zugreifen, andere aber nicht.

OPEN-Unterstützung zur gemeinsamen Nutzung in NFS-Version 4

Das Protokoll der NFS-Version 4 bietet mehrere Modi zum gemeinsamen Dateizugriff, die der Client verwenden kann, um den Dateizugriff anderer Clients zu steuern. Ein Client kann Folgendes definieren:

- DENY_NONE-Modus – andere Clients erhalten Lese- und Schreibzugriff auf eine Datei.
- DENY_READ-Modus – anderen Clients wird der Lesezugriff auf eine Datei verweigert.
- DENY_WRITE-Modus – anderen Clients wird der Schreibzugriff auf eine Datei verweigert.
- DENY_BOTH-Modus – anderen Clients wird der Lese- und Schreibzugriff auf eine Datei verweigert.

Diese Modi für den gemeinsamen Dateizugriff werden vom Server der NFS-Version 4 von Solaris vollständig implementiert. Wenn ein Client versucht, eine Datei auf eine Art und Weise zu öffnen, die mit dem aktuellen Modus zum gemeinsamen Dateizugriff in Konflikt steht, verweigert der Server diesen Vorgang, wodurch der Vorgang fehlschlägt. Wenn ein solcher Versuch bei der Einleitung von Öffnungs- oder Erstellungsvorgängen fehlschlägt, empfängt der Client der NFS-Version 4 einen Protokollfehler. Dieser Fehler wird dem Anwendungsfehler EACCES zugeordnet.

Obwohl das Protokoll mehrere Modi zum gemeinsamen Dateizugriff bietet, ist dies derzeit beim Öffnungsvorgang in Solaris nicht der Fall. Wenn eine Datei geöffnet wird, kann ein Client der NFS-Version 4 von Solaris nur den DENY_NONE-Modus verwenden.

Obwohl der Systemaufruf fcntl einen F_SHARE-Befehl verwendet, um den gemeinsamen Dateizugriff zu steuern, können die fcntl-Befehle mit NFS-Version 4 nicht richtig implementiert werden. Wenn Sie diese fcntl-Befehle auf einem Client der NFS-Version 4 anwenden, gibt der Client den Fehler EAGAIN an die Anwendung zurück.

Delegierung in NFS-Version 4

NFS-Version 4 bietet sowohl Client- als auch Serverunterstützung für die Delegierung. Delegierung ist ein Verfahren, bei dem ein Server die Verwaltung einer Datei an einen Client delegiert. Ein Server kann beispielsweise einem Client eine Lese- oder Schreibdelegierung gewähren. Lesedelegierungen können mehreren Clients gleichzeitig gewährt werden, da diese Delegierungen nicht miteinander in Konflikt stehen. Eine Schreibdelegierung kann nur einem Client gewährt werden, da eine solche Delegierung mit Zugriffsvorgängen, die von anderen Clients ausgeführt werden, in Konflikt geraten können. Wenn der Client eine Schreibdelegierung besitzt, sendet er keine Vorgänge an den Server, wenn ihm der exklusiver Zugriff auf eine Datei garantiert wird. Der Client sendet auch dann keine Vorgänge an den Server, wenn er eine Schreibdelegierung besitzt. Der Grund dafür ist der, dass der Server gewährleistet, dass kein Client die Datei im Schreibmodus öffnen kann. Die Delegierung hat den Zweck, die Vorgänge zwischen dem Server und dem Client bedeutend zu verringern. Dies hat auch zur Folge, dass der Netzwerkverkehr verringert wird und die Leistung von Clients und

Servern verbessert wird. Beachten Sie jedoch, dass der Grad der Leistungssteigerung davon abhängt, welche Dateien von einer Anwendung verwendet und wie stark das Netzwerk und der Server belastet werden.

Die Entscheidung, ob eine Delegierung gewährt wird, wird allein vom Server getroffen. Von einem Client wird keine Delegierung angefordert. Die vom Server getroffenen Entscheidungen bezüglich einer Delegierung begründen sich auf den Dateizugriffsmustern. Wenn kurze Zeit zuvor von verschiedenen Clients im Schreibmodus auf eine Datei zugegriffen wurde, gewährt der Server eventuell keine Delegierung. Der Grund ist der, dass dieses Zugriffsmuster auf potenzielle zukünftige Konflikte hindeutet.

Ein Konflikt entsteht, wenn ein Client auf eine Art und Weise auf eine Datei zugreift, die mit der Delegierung in Widerspruch steht, die vor kurzem für den Zugriff auf diese Datei gewährt wurde. Wenn ein Client beispielsweise im Besitz einer Schreibdelegierung für eine Datei ist und die Datei von einem zweiten Client geöffnet wird, um Lese- oder Schreibzugriff zu erhalten, widerruft der Server die Schreibdelegierung des ersten Clients. Ein ähnlicher Vorgang findet statt, wenn ein Client im Besitz einer Lesedelegierung ist und ein anderer Client dieselbe Datei öffnet, um Schreibzugriff zu erhalten: Der Server widerruft die Lesedelegierung. In beiden Fällen wird dem zweiten Client keine Delegierung gewährt, weil ein Konflikt entstanden ist. Sobald ein Konflikt ensteht, verwendet der Server einen Callback-Mechanismus, um den Client zu kontaktieren, der im Besitz der Delegierung ist. Nachdem der Client diesen Callback empfangen hat, sendet er die aktualisierten Daten der Datei an den Server und gibt die Delegierung zurück. Wenn der Client nicht auf den erneuten Aufruf antwortet, widerruft der Server die Delegierung. In solchen Fällen lehnt der Server alle Vorgänge ab, die vom Client für diese Datei angefordert werden, und der Client meldet, dass die angeforderten Vorgänge fehlgeschlagen sind. Fehlgeschlagenen Vorgänge dieser Art werden der Anwendung als `E/A`-Fehler gemeldet. Um diese Fehler zu beheben, muss die Datei geschlossen und dann wieder geöffnet werden. Fehler, die aus widerrufenen Delegierungen resultieren, können auftreten, wenn eine Netzwerkpartition zwischen dem Client und dem Server vorhanden ist, während der Client im Besitz einer Delegierung ist.

Beachten Sie, dass ein Server keine Zugriffskonflikte löst, die aus einer Datei resultieren, die auf einem anderen Server gespeichert ist. Aus diesem Grund löst ein NFS-Server nur Konflikte, die aus Dateien resultieren, die von ihm selbst gespeichert werden. Außerdem kann ein Server, der auf Konflikte auftwortet, die von Clients verursacht werden, auf denen verschiedene NFS-Versionen ausgeführt werden, nur an den Client erneute Aufrufe senden, auf dem die NFS-Version 4 ausgeführt wird. Ein NFS-Server kann keine erneuten Aufrufe für Clients einleiten, auf denen frühere Versionen von NFS ausgeführt werden.

Die Erkennung von Konflikten gestaltet sich unterschiedlich. Anders als in NFS-Version 4 wird ein Konflikt erst dann erkannt, wenn der Client versucht, eine Datei zu lesen, zu beschreiben oder zu sperren, da bei den Versionen 2 und 3 kein offenes Verfahren verwendet wird. Die Antwort des Servers auf diese Konflikte fällt ebenfalls unterschiedlich aus. Beispiel:

- In NFS-Version 3 gibt der Server den Fehler `JUKEBOX` zurück, wodurch der Client veranlasst wird, die Zugriffsanforderung auszusetzen und es zu einem späteren Zeitpunkt erneut zu versuchen. Der Client gibt die Meldung `File unavailable` (Datei nicht verfügbar) aus.
- Da in NFS-Version 2 keine Entsprechung für den Fehler `JUKEBOX` vorhanden ist, antwortet der Server nicht, wodurch der Client zunächst wartet und dann erneut versucht, den Vorgang auszuführen. Der Client gibt die Meldung `NFS server not responding` (NFS-Server antwortet nicht) aus.

Dieser Zustand ist beendet, sobald der Delegierungskonflikt gelöst ist.

Die Serverdelegierung ist standardmäßig aktiviert. Sie können die Delegierung deaktivieren, indem Sie die `/etc/default/nfs` -Datei modifizieren. Informationen zur Verfahrensweise finden Sie unter „So wählen Sie andere NFS-Versionen auf einem Server aus“ auf Seite 99.

Für die Clientdelegierung sind keine Schlüsselwörter erforderlich. Der Callback-Dämon der NFS-Version 4, `nfs4cbd`, stellt einen Callback-Service auf dem Client bereit. Dieser Dämon wird automatisch gestartet, wenn eine Einhängung für NFS-Version 4 aktiviert wird. Der Client übermittelt standardmäßig die Callback-Informationen an den Server, die für alle Internetübertragungen benötigt werden, die in der `/etc/netconfig` -Systemdatei aufgelistet sind. Bitte beachten Sie: Wenn der Client für IPv6 aktiviert ist und die IPv6-Adresse für den Namen des Clients nicht bestimmt werden kann, akzeptiert der Callback-Dämon IPv6-Verbindungen.

Der Callback-Dämon verwendet eine vorübergehende Programmnummer und eine dynamisch zugewiesene Portnummer. Diese Informationen werden dem Server zur Verfügung gestellt, und der Server prüft den Callback-Pfad, bevor er Delegierungen zulässt. Wenn die Prüfung des Callback-Pfads nicht erfolgreich war, gewährt der Server keine Delegierungen. Dies ist das einzige nach außen hin erkennbare Verhalten.

Bitte beachten Sie: Da die Callback-Informationen in eine Anforderung der NFS-Version 4 eingebettet sind, kann der Server den Client nicht über ein Gerät kontaktieren, das NAT (Network Address Translation) verwendet. Der Callback-Dämon verwendet zudem eine dynamische Portnummer. Aus diesem Grund ist der Server eventuell nicht in der Lage, eine Firewall zu überwinden, was auch dann der Fall ist, wenn die betreffende Firewall normalen NFS-Verkehr an Port 2049 zulässt. In solchen Fällen gewährt der Server keine Delegierungen.

Zugriffskontrolllisten (ACLs) und `nfsmapid` in NFS-Version 4

Eine Zugriffskontrollliste (ACL) bietet mehr Sicherheit für Dateien, da dem Eigentümer einer Datei ermöglicht wird, Dateiberechtigungen für den Dateieigentümer, die Gruppe und weitere

Benutzer und Gruppen zu definieren. Zugriffskontrolllisten werden auf dem Server und dem Client definiert, indem der Befehl `setfacl` verwendet wird. Weitere Informationen finden Sie auf der Manpage `setfacl(1)`. In der NFS-Version 4 wird der ID-Mapper `nfsmapid` verwendet, um Benutzer- oder Gruppen-IDs in Zugriffssteuerungslisteneinträgen auf einem Server den Benutzer- oder Gruppen-IDs in Zugriffssteuerungslisteneinträgen auf einem Client zuzuordnen. Die Zuordnung erfolgt auch in umgekehrter Richtung. Die Benutzer- und Gruppen-IDs in den Einträgen der Zugriffssteuerungsliste müssen sowohl auf dem Client als auch auf dem Server vorhanden sein.

Gründe für eine fehlgeschlagene ID-Zuordnung

Eine ID-Zuordnung kann aus folgenden Gründen fehlschlagen:

- Wenn ein Benutzer, der in einem Zugriffssteuerungslisteneintrag auf einem Server angegeben ist, oder eine Gruppe, die in einem solchen Eintrag angegeben ist, nicht einem gültigen Benutzer oder einer gültigen Gruppe auf einem Client zugeordnet werden kann, wird dem Benutzer bzw. der Gruppe nicht erlaubt, die Zugriffssteuerungsliste auf dem Client zu lesen.

  Wenn Sie beispielsweise den Befehl `ls -lv` oder den Befehl `ls -lV` ausgeben, erhalten Sie die Fehlermeldung "`Permission denied`"(Zugriff verweigert). Diese Fehlermeldung bezieht sich auf die Dateien mit Benutzer- oder Gruppen-ID-Einträgen in der Zugriffssteuerungsliste, die der Server nicht dem Client zuordnen kann. Der ID-Mapper konnte einen Benutzer oder eine Gruppe in der Zugriffssteuerungsliste nicht zuordnen. Wenn der ID-Mapper einen Benutzer oder eine Gruppe zuordnen kann, steht ein Pluszeichen (+) hinter den Berechtigungen in der Dateiliste, die durch `ls -l` erstellt wird. Beispiel:

  ```
  % ls -l
  -rw-r--rw-+   1 luis    staff      11968 Aug 12  2005 foobar
  ```

  Der Befehl `getfacl` kann die Fehlermeldung "`Permission denied`" (Zugriff verweigert) aus dem gleichen Grund zurückgeben. Weitere Informationen zu diesem Befehl finden Sie auf der Manpage `getfacl(1)`.
- Wenn die Benutzer- oder Gruppen-ID in einem Zugriffssteuerungslisteneintrag, der für den Client definiert ist, keiner gültigen Benutzer- oder Gruppen-ID auf dem Server zugeordnet werden kann, kann die Ausführung des Befehls `setfacl` oder des Befehls `chmod` fehlschlagen, wodurch die Fehlermeldung "`Permission denied`" (Zugriff verweigert) zurückgegeben wird.
- Wenn die NFSMAPID_DOMAIN-Werte des Clients und des Servers nicht übereinstimmen, schlägt die ID-Zuordnung fehl. Weitere Informationen finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144.

Vermeiden von ID-Zuordnungsproblemen mit Zugriffssteuerungslisten

Um ID-Zuordnungsprobleme zu vermeiden, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass der Wert für NFSMAPID_DOMAIN in der `/etc/default/nfs`-Datei korrekt angegeben ist.
- Stellen Sie sicher, dass alle Benutzer- und Gruppen-IDs in den Einträgen der Zugriffssteuerungsliste sowohl auf dem Client als auch auf dem Server der NFS-Version 4 vorhanden sind.

Prüfen auf nicht zugeordnete Benutzer- oder Gruppen-IDs

Um festzustellen, ob ein Benutzer oder eine Gruppe nicht auf dem Server oder Client zugeordnet werden kann, verwenden Sie das folgende Skript:

```
#! /usr/sbin/dtrace -Fs

sdt:::nfs4-acl-nobody
{
     printf("validate_idmapping: (%s) in the ACL could not be mapped!",
stringof(arg0));
}
```

Hinweis – Der Probename, der in diesem Skript verwendet wird, ist eine Schnittstelle, die später geändert werden kann. Weitere Informationen finden Sie unter „Stabilitätsstufen“ in *Handbuch zur dynamischen Ablaufverfolgung in Solaris*.

Zusätzliche Informationen zu Zugriffssteuerungslisten oder nfsmapid

Siehe Folgendes:

- „Schützen von UFS-Dateien mit ACLs (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*
- Kapitel 8, „Schützen von Oracle Solaris ZFS-Dateien mit Zugriffssteuerungslisten und Attributen“ in *Oracle Solaris ZFS-Administrationshandbuch*
- „`nfsmapid`-Dämon“ auf Seite 151

UDP- und TCP-Aushandlung

Während der Initiierung wird auch das Transportprotokoll ausgehandelt. Standardmäßig wird das erste verbindungsorientierte Transportprotokoll ausgewählt, das sowohl auf dem Client als auch auf dem Server unterstützt wird. Wird die Auswahl nicht erfolgreich durchgeführt, wird das erste verbindungslose Transportprotokoll verwendet. Die auf einem System unterstützten

Transportprotokolle werden in `/etc/netconfig` aufgelistet. Das von dieser Version unterstützte verbindungsorientierte Transportprotokoll ist TCP. UDP ist das verbindungslose Transportprotokoll.

Wenn sowohl die NFS-Protokollversion als auch das Transportprotokoll durch die Aushandlung festgelegt werden, hat die NFS-Protokollversion Vorrang vor dem Transportprotokoll. Das Protokoll der NFS-Version 3, das UDP verwendet, hat Vorrang vor dem Protokoll der NFS-Version 2, das TCP verwendet. Sie können sowohl die NFS-Protokollversion als auch das Transportprotokoll manuell auswählen, indem Sie den Befehl `mount` verwenden. Weitere Informationen finden Sie auf der Manpage `mount_nfs(1M)`. In den meisten Fällen sollten Sie die Aushandlung zulassen, damit die besten Optionen ausgewählt werden.

Aushandlung der Dateiübertragungsgröße

Mit der Dateiübertragungsgröße wird die Größe der Puffer festgelegt, die verwendet werden, wenn Daten zwischen dem Client und dem Server übertragen werden. Im Allgemeinen sind höherwertige Übertragungsgrößen vorzuziehen. Das Protokoll der NFS-Version 3 hat eine unbegrenzte Übertragungsgröße. Ab Solaris 2.6 bietet die Software jedoch eine standardmäßige Puffergröße von 32 KB. Der Client kann zum Transport der Einhängung eine kleinere Übertragungsgröße anbieten. In den meisten Fällen ist dies jedoch nicht nötig.

Die Übertragungsgröße wird nicht mit Systemen ausgehandelt, die das Protokoll der NFS-Version 2 verwenden. Dementsprechend wird die maximale Übertragungsgröße auf 8 KB gesetzt.

Sie können die Optionen `-rsize` und `-wsize` verwenden, um die Übertragungsgröße manuell mithilfe des Befehls `mount` festzulegen. Eventuell müssen Sie die Übertragungsgröße für manche PC-Clients verringern. Sie können die Übertragungsgröße aber auch erhöhen, wenn die Konfiguration des NFS-Servers die Verwendung höherwertiger Übertragungsgrößen zulässt.

Hinweis – Ab Solaris 10 wurden die Beschränkungen der leitungsgebundenen Übertragungsgrößen gelockert. Die Übertragungsgröße basiert nun auf den Funktionen des zugrunde liegenden Transportmechanismus. Das NFS-Übertragungsgrenze für UDP liegt beispielsweise weiterhin bei 32 KB. Da die Datagramm-Grenzwerte für UDP aber nicht auf das Streaming-Protokoll TCP zutreffen, wurde die maximale Übertragungsgröße bei Verwendung von TCP auf 1 MB erhöht.

Einhängen von Dateisystemen

Die folgende Beschreibung bezieht sich auf Einhängungen mit NFS-Version 3. Im Einhängeprozess der NFS-Version 4 sind weder der Portmap-Service noch das `MOUNT`-Protokoll enthalten.

Wenn ein Client ein Dateisystem von einem Server einhängen muss, muss der Client zunächst eine Dateizugriffsroutine vom Server abrufen. Die Dateizugriffsroutine muss zum Dateisystem passen. Dieses Verfahren erfordert die Durchführung mehrerer Transaktionen zwischen dem Client und dem Server. In diesem Beispiel versucht der Client, das auf dem Server befindliche System `/home/terry` einzuhängen. Nach dieser Transaktion wird eine `snoop`-Ablaufverfolgung durchgeführt.

```
client -> server PORTMAP C GETPORT prog=100005 (MOUNT) vers=3 proto=UDP
server -> client PORTMAP R GETPORT port=33492
client -> server MOUNT3 C Null
server -> client MOUNT3 R Null
client -> server MOUNT3 C Mount /export/home9/terry
server -> client MOUNT3 R Mount OK FH=9000 Auth=unix
client -> server PORTMAP C GETPORT prog=100003 (NFS) vers=3 proto=TCP
server -> client PORTMAP R GETPORT port=2049
client -> server NFS C NULL3
server -> client NFS R NULL3
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

Während dieser Ablaufverfolgung fordert der Client zunächst die Einhängeportnummer vom Portmap-Service auf dem NFS-Server an. Nachdem der Client die Einhängeportnummer (`33492`) empfangen hat, wird diese verwendet, um festzustellen, ob der Service auf dem Server verfügbar ist. Nachdem der Client festgestellt hat, dass an der betreffenden Portnummer ein Service vorhanden ist, kann er eine Einhängungsanforderung versenden. Wenn der Server auf diese Anforderung antwortet, stellt der Server die Dateizugriffsroutine für das Dateisystem (`9000`) bereit, das eingehängt werden soll. Der Client fordert dann die NFS-Portnummer an. Wenn der Client die Nummer vom Server erhalten hat, prüft er die Verfügbarkeit des NFS-Service (`nfsd`). Außerdem fordert der Client NFS-Informationen zum Dateisystem an, das die Dateizugriffsroutine verwendet.

Im folgenden Beispiel hängt der Client ein Dateisystem mithilfe der Option `public` ein.

```
client -> server NFS C LOOKUP3 FH=0000 /export/home9/terry
server -> client NFS R LOOKUP3 OK FH=9000
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

Durch Verwendung der standardmäßigen Routine für den Zugriff auf öffentliche Dateien (`0000`) werden alle Transaktionen übersprungen, die zum Abrufen von Informationen vom Portmap-Service und zur Bestimmung der NFS-Portnummer dienen.

Hinweis – NFS-Version 4 bietet Unterstützung für temporäre Dateizugriffsroutinen. Weitere Informationen finden Sie unter „Temporäre Dateizugriffsroutinen in NFS-Version 4“ auf Seite 191.

Funktionsweise der Option `-public` und der NFS-URLs beim Einhängen

Die Verwendung der Option `-public` kann zum Fehlschlagen einer Einhängung führen. Die Situation kann auch kompliziert werden, wenn eine NFS-URL hinzugefügt wird. In der folgenden Liste wird beschrieben, wie ein Dateisystem eingehängt wird, wenn die folgenden Optionen verwendet werden:

Public option with NFS URL – erzwingt die Verwendung der Routine für den Zugriff auf öffentliche Dateien. Das Einhängen schlägt fehl, wenn die Routine für den Zugriff auf öffentliche Dateien nicht unterstützt wird.

Public option with regular path – erzwingt die Verwendung der Routine für den Zugriff auf öffentliche Dateien. Das Einhängen schlägt fehl, wenn die Routine für den Zugriff auf öffentliche Dateien nicht unterstützt wird.

NFS URL only – die Routine für den Zugriff auf öffentliche Dateien wird verwendet, wenn diese Dateizugriffsroutine auf dem NFS-Server aktiviert ist. Schlägt die Einhängung fehl, wenn die Routine für den Zugriff auf öffentliche Dateien verwendet wird, versuchen Sie, die Einhängung mit dem `MOUNT`-Protokoll durchzuführen.

Regular path only – verwenden Sie nicht die Routine für den Zugriff auf öffentliche Dateien. Das `MOUNT`-Protokoll wird verwendet.

Clientseitiges Failover

Durch Verwendung des clientseitigen Failover hat ein NFS-Client Kenntnis von vielen Servern, die dieselben Daten zur Verfügung stellen. Dadurch kann ein alternativer Server verwendet werden, wenn der aktuelle Server nicht verfügbar ist. Das Dateisystem kann eventuell nicht mehr zur Verfügung stehen, wenn Folgendes geschieht:

- Ein Server, mit dem das Dateisystem verbunden ist, stürzt ab.
- Der Server ist überlastet.
- Ein Netzwerkfehler tritt auf.

Unter diesen Bedingungen ist das Failover für den Benutzer normalerweise transparent. Das Failover kann jederzeit stattfinden, ohne die Prozesse zu unterbrechen, die auf dem Client ausgeführt werden.

Ein Failover erfordert, dass das Dateisystem mit Schreibschutz eingehängt ist. Die Dateisysteme müssen identisch sein, damit das Failover erfolgreich ausgeführt werden kann. Eine Beschreibung, wann ein Dateisystem identisch ist, finden Sie unter „Was ist ein repliziertes Dateisystem?“ auf Seite 203. Ein statisches Dateisystem oder ein Dateisystem, das nur selten geändert wird, eignet sich am besten für ein Failover.

Sie können CacheFS und clientseitiges Failover nicht für dieselbe NFS-Einhängung verwenden. Für jedes CacheFS-Dateisystem werden zusätzliche Informationen gespeichert. Da diese Informationen während des Failover nicht aktualisiert werden können, kann nur eine dieser Funktionen verwendet werden, wenn ein Dateisystem eingehängt wird.

Wie viele Replikationen für jedes Dateisystem bereitgestellt werden müssen, hängt von zahlreichen Faktoren ab. Idealerweise sollten Sie mindestens über zwei Server verfügen. Jeder Server sollte mehrere Teilnetze unterstützen. Dies ist effizienter, als jeweils einen Server pro Teilnetz einzusetzen. Das Verfahren erfordert, dass jeder gelistete Server geprüft wird. Aus diesem Grund geht das Einhängen umso langsamer vonstatten, je mehr Server gelistet sind.

Failover-Terminologie

Um diesen Prozess zu verstehen, müssen Sie zwei Begriffe kennen:

- *Failover* – Die Auswahl eines Servers aus einer Liste von Servern, die ein repliziertes Dateisystem unterstützen. Normalerweise wird der nächste Server in der sortierten Liste verwendet, sofern er antwortet.
- *Neuzuordnung* – Die Verwendung eines neuen Servers. Durch die normale Verwendung wird der Pfadname für jede aktive Datei des Remote-Dateisystems von den Clients gespeichert. Während der Neuzuordnung werden diese Pfadnamen evaluiert, um die Dateien auf dem neuen Server zu platzieren.

Was ist ein repliziertes Dateisystem?

Für die Zwecke des Failover wird ein Dateisystem als *Replikation* bezeichnet, wenn jede Datei gleich groß ist und die gleiche Größe und den gleichen Typ aufweist, wie das ursprüngliche Dateisystem. Berechtigungen, Erstellungdaten und andere Dateiattribute werden nicht berücksichtigt. Wenn die Dateigröße oder die Dateitypen unterschiedlich sind, schlägt die Neuzuweisung fehl, und der Prozess bleibt hängen, bis der alte Server wieder zur Verfügung steht. In NFS-Version 4 ist das Verhalten unterschiedlich. Lesen Sie dazu „Clientseitiges Failover in NFS-Version 4“ auf Seite 204.

Sie können ein repliziertes Dateisystem verwalten, indem Sie `rdist`, `cpio` oder einen anderen Dateiübertragungsmechanismus verwenden. Da durch die Aktualisierung der replizierten Dateisysteme Inkonsistenzen verursacht werden, sollten folgende Sicherheitsmaßnahmen getroffen werden, um optimale Ergebnisse zu erzielen:

- Umbenennen der alten Dateiversion vor dem Installieren einer neuen Version
- Ausführen der Aktualisierungen in der Nacht, wenn die Clientauslastung niedrig ist
- Durchführung möglichst kleiner Aktualisierungen
- Minimierung der Anzahl von Kopien

Failover und NFS-Sperrung

Manche Softwarepakete erfordern eine Sperrung des Lesezugriffs auf Dateien. Um eine Beschädigung dieser Produkte zu vermeiden, werden Sperrungen des Lesezugriffs auf schreibgeschützte Dateisysteme zugelassen. Sie sind allerdings nur auf der Clientseite sichtbar. Die Sperren bleiben bei einer Neuzuordnung bestehen, da dem Server diese Sperren nicht bekannt sind. Da die Dateien nicht geändert werden, müssen sie auf der Serverseite nicht gesperrt werden.

Clientseitiges Failover in NFS-Version 4

Wenn in NFS-Version 4 eine Replikation nicht bereitgestellt werden kann, weil die Dateigrößen unterschiedlich sind oder die Dateitypen nicht übereinstimmen, geschieht Folgendes:

- Die Datei wird als gesperrt gekennzeichnet.
- Eine Warnung wird ausgegeben.
- Die Anwendung empfängt einen Systemaufruffehler.

Hinweis – Wenn Sie die Anwendung neu starten und erneut versuchen, auf die Datei zuzugreifen, sollten keine Probleme auftreten.

In NFS-Version 4 werden keine Replikationsfehler bei Verzeichnissen von unterschiedlicher Größe angezeigt. In früheren Versionen von NFS wurde in diesem Fall ein Fehler gemeldet, der den Neuzuordnungsprozess behindert.

Wenn in NFS-Version 4 ein Verzeichnis nicht gelesen werden kann, wird der Vorgang vom nächsten gelisteten Server ausgeführt. In früheren Versionen von NFS führten nicht erfolgreiche Lesevorgänge dazu, dass die Neuzuordnung fehlschlug und der Prozess hing, bis der ursprüngliche Server wieder verfügbar war.

Große Dateien

Das Betriebssystem unterstützt Dateien mit einer Größe von über 2 GB. UFS-Dateisysteme werden standardmäßig mit der Option `-largefiles` eingehängt, um die neue Funktion zu unterstützen. Lesen Sie bei Bedarf dazu „So deaktivieren Sie große Dateien auf einem NFS-Server“ auf Seite 93.

Wenn das Dateisystem des Servers mithilfe der Option `-largefiles` eingehängt wird, kann ein Solaris 2.6-NFS-Client auf große Dateien zugreifen, ohne dass Änderungen erforderlich sind. Jedoch können diese großen Dateien nicht mithilfe von allen Solaris 2.6-Befehlen verarbeitet werden. Eine Liste der Befehle, die in Verbindung mit großen Dateien verwendet werden können, finden Sie unter `largefile(5)`. Clients, die das Protokoll der NFS-Version 3 mit den Erweiterungen für große Dateien nicht unterstützen, können nicht auf große Dateien zugreifen. Obwohl Clients, auf denen Solaris 2.5 ausgeführt wird, das Protokoll der NFS-Version 3 verwenden können, unterstützt die Version nicht die Verarbeitung großer Dateien.

Funktionsweise der NFS-Serverprotokollierung

Die NFS-Serverprotokollierung stellt Datensätze der NFS-Lese- und Schreibvorgänge sowie der Vorgänge bereit, die zum Modifizieren des Dateisystems dienen. Diese Daten können verwendet werden, um den Zugriff auf Informationen zu verfolgen. Außerdem bieten Datensätze eine Möglichkeit, die Nachfrage nach diesen Informationen zu messen.

Wenn auf ein Dateisystem, für das die Protokollierung aktiviert ist, zugegriffen wird, schreibt der Kernel die Raw-Daten in eine Pufferdatei. In diesen Daten ist Folgendes enthalten:

- Ein Zeitstempel
- Die Client-IP-Adresse
- Die UID des Anforderers
- Die Dateizugriffsroutine des Datei- oder Verzeichnisobjekts, auf das zugegriffen wird
- Die Art des ausgeführten Vorgangs

Der Dämon `nfslogd` konvertiert diese Raw-Daten in ASCII-Datensätze, die in Protokolldateien gespeichert werden. Während der Konvertierung werden die IP-Adressen in Hostnamen und die UIDs in Anmeldenamen umgewandelt, wenn der aktivierte Name Service Übereinstimmungen finden kann. Außerdem werden die Dateizugriffsroutinen in Pfadnamen konvertiert. Um die Konvertierung durchzuführen, verfolgt der Dämon die Dateizugriffsroutinen und speichert die Informationen in einer separaten Dateizugriffsroutine-zu-Pfad-Tabelle. Dadurch muss der Pfad nicht jedesmal aufs Neue ermittelt werden, wenn auf eine Dateizugriffsroutine zugegriffen wird. Da keine Änderungen

an den Zuordnungen in der Dateizugriffsroutine-zu-Pfad-Tabelle vorgenommen werden, wenn `nfslogd` deaktiviert ist, müssen Sie dafür sorgen, dass der Dämon weiterhin ausgeführt wird.

Hinweis – Die Serverprotokollierung wird nicht in NFS-Version 4 unterstützt.

Funktionsweise des WebNFS-Service

Der WebNFS-Service stellt den Clients Dateien in einem Verzeichnis zur Verfügung, indem eine Routine für den Zugriff auf öffentliche Dateien verwendet wird. Eine Dateizugriffsroutine ist eine vom Kernel generierte Adresse, die zur Angabe einer Datei für NFS-Clients dient. Die *Routine für den Zugriff auf öffentliche Dateien* hat einen vordefinierten Wert, sodass der Server keine Dateizugriffsroutine für den Client generieren muss. Durch die Fähigkeit, diese vordefinierte Dateizugriffsroutine zu verwenden, wird der Netzwerkverkehr verringert, da die Verwendung des `MOUNT`-Protokolls entfällt. Diese Fähigkeit beschleunigt zudem die clientbezogenen Prozesse.

Die Routine für den Zugriff auf öffentliche Dateien auf einem NFS-Server wird standardmäßig im Root-Dateisystem erstellt. Dieser standardmäßige Vorgang gewährleistet den WebNFS-Zugriff auf alle Clients, die bereits über Einhängeberechtigungen auf dem Server verfügen. Sie können die Routine für den Zugriff auf öffentliche Dateien ändern, um auf ein beliebiges Dateisystem mithilfe des Befehls `share` zu verweisen.

Wenn der Client über die Dateizugriffsroutine für das Dateisystem verfügt, wird ein `LOOKUP`-Vorgang ausgeführt, um die Dateizugriffsroutine für die Datei zu bestimmen, auf die zugegriffen wird. Das NFS-Protokoll ermöglicht die Evaluierung von jeweils nur einer Pfadnamenkomponente. Jede weitere Verzeichnishierarchieebene erfordert einen weiteren `LOOKUP`-Vorgang. Ein WebNFS-Server kann den gesamten Pfadnamen mithilfe einer einzelnen Mehrkomponenten-Suchtransaktion evaluieren, wenn der `LOOKUP`-Vorgang in Relation zur Routine für den Zugriff auf öffentliche Dateien steht. Mehrkomponenten-Suchvorgänge ermöglichen dem Webserver, die Dateizugriffsroutine für die gewünschte Datei bereitzustellen, ohne die Dateizugriffsroutinen für jede Verzeichnisebene im Pfadnamen auszutauschen.

Außerdem kann ein NFS-Client gleichzeitige Downloads über eine einzige TCP-Verbindung einleiten. Diese Verbindung ermöglicht einen schnellen Zugriff ohne zusätzliche Belastung des Servers durch das Einrichten mehrerer Verbindungen. Obwohl Webbrowseranwendungen das gleichzeitige Herunterladen mehrerer Dateien unterstützen, hat jede Datei eine eigene Verbindung. Durch die Verwendung einer Verbindung kann die WebNFS-Software die Mehrbelastung des Servers verringern.

Wenn die letzte Komponente des Pfadnamens eine symbolische Verknüpfung zu einem anderen Dateisystem ist, kann der Client auf die Datei zugreifen, wenn er bereits über Zugriff durch normale NFS-Aktivitäten verfügt.

Normalerweise wird eine NFS-URL in Relation zur Routine für den Zugriff auf öffentliche Dateien evaluiert. Die Evaluierung kann geändert werden, damit sie in Relation zum Root-Dateisystem des Servers steht, indem ein zusätzlicher Schrägstrich an den Anfang des Pfads gesetzt wird. Die ibeiden NFS-URLs in diesem Beispiel sind äquivalent, wenn die Routine für den Zugriff auf öffentliche Dateien im `/export/ftp`-Dateisystem bereitgestellt ist.

```
nfs://server/junk
nfs://server//export/ftp/junk
```

Hinweis – Das Protokoll der NFS-Version 4 ist dem WebNFS-Service vorzuziehen. In der NFS-Version 4 sind sämtliche Sicherheitsaushandlungen integriert, die in das MOUNT-Protokoll und den WebNFS-Service aufgenommen wurden.

Funktionsweise der WebNFS-Sicherheitsaushandlung

Der NFS-Service stellt ein neues Protokoll bereit, das WebNFS-Clients ermöglicht, einen bestimmten Sicherheitsmechanismus mit einem WebNFS-Server auszuhandeln. Das neue Protokoll verwendet für die Sicherheitsaushandlung eine Mehrkomponenten-Suche, bei der es sich um eine Erweiterung der Mehrkomponenten-Suche handelt, die in früheren Versionen des WebNFS-Protokolls verwendet wurde.

Der WebNFS-Client initiiert den Prozess, indem er mithilfe der Routine für den Zugriff auf öffentliche Dateien eine normale Mehrkomponenten-Suche anfordert. Da dem Client nicht bekannt ist, wie der Pfad durch den Server geschützt wird, wird der standardmäßige Sicherheitsmechanismus verwendet. Wenn der standardmäßige Sicherheitsmechanismus nicht ausreicht, antwortet der Server mit einem `AUTH_TOOWEAK`-Fehler. Dadurch wird angezeigt, dass der Mechanismus nicht gültig ist. Der Client muss einen wirkungsvolleren Standardmechanismus verwenden.

Nachdem der Client den `AUTH_TOOWEAK`-Fehler empfangen hat, sendet er eine Anforderung an den Server, um festzustellen, welche Sicherheitsmechanismen erforderlich sind. Wenn die Anforderung erfolgreich durchgeführt wird, antwortet der Server mit einer Feldgruppe von Sicherheitsmechanismen, die für den angegebenen Pfad erforderlich sind. Je nach Größe der Feldgruppe der Sicherheitsmechanismen führt der Client weitere Anforderungen aus, um die vollständige Feldgruppe abzurufen. Wenn der Server die WebNFS-Sicherheitsaushandlung nicht unterstützt, schlägt die Anforderung fehl.

Nach einer erfolgreich durchgeführten Anforderung wählt der WebNFS-Client den ersten Sicherheitsmechanismus aus der Feldgruppe aus, die vom Client unterstützt wird. Der Client gibt dann eine normale Mehrkomponenten-Suchanforderung aus, indem er die ausgewählten Sicherheitsmechanismen verwendet, um die Dateizugriffsroutine abzurufen. Alle nachfolgenden NFS-Anforderungen werden mithilfe des ausgewählten Sicherheitsmechanismus und der Dateizugriffsroutine durchgeführt.

Hinweis – Das Protokoll der NFS-Version 4 ist dem WebNFS-Service vorzuziehen. In der NFS-Version 4 sind sämtliche Sicherheitsaushandlungen integriert, die in das MOUNT-Protokoll und den WebNFS-Service aufgenommen wurden.

WebNFS-Beschränkungen bei Verwendung eines Webbrowsers

Viele Funktionen, die von einer Website bereitgestellt werden, die HTTP verwendet, werden von der WebNFS-Software nicht unterstützt. Diese Unterschiede sind auf die Tatsache zurückzuführen, dass der NFS-Server die Datei lediglich sendet, wodurch bestimmte Verarbeitungsvorgänge vom Client ausgeführt werden müssen. Wenn eine Website sowohl für den WebNFS- als auch für den HTTP-Zugriff konfiguriert werden muss, ist Folgendes zu berücksichtigen:

- Bei NFS-Suchvorgängen werden keine CGI-Skripten ausgeführt. Aus diesem Grund kann ein Dateisystem mit einer aktiven Website, auf der viele Skripten verwendet werden, eventuell nicht mithilfe von NFS durchsucht werden.
- Der Browser startet möglicherweise verschiedene Viewer, um Dateien in verschiedenen Dateiformaten zu verarbeiten. Durch den Zugriff auf diese Dateien über eine NFS-URL wird ein externer Viewer gestartet, wenn der Dateityp durch den Dateinamen bestimmt werden kann. Der Browser erkennt normalerweise alle Dateinamenserweiterungen für standardmäßige MIME-Typen, wenn eine NFS-URL verwendet wird. Die WebNFS-Software prüft nicht den Inhalt der Datei, um den Dateityp zu bestimmen. Darum kann ein Dateiname nur anhand der Dateinamenserweiterung bestimmt werden.
- In NFS-Suchvorgängen können keine serverseitigen ImageMaps (anklickbare Bilder) verwendet werden. Es können aber clientseitige ImageMaps (anklickbare Bilder) verwendet werden, weil die URLs durch Speicherorte definiert werden. Es ist keine weitere Anwort des Dokumentservers erforderlich.

Sicheres NFS-System

Die NFS-Umgebung ist eine effiziente und bequeme Methode zur gemeinsamen Nutzung von Dateisystemen in einem Netzwerk, das aus verschiedenen Computerarchitekturen und Betriebssystemen besteht. Die Funktionen, die eine reibungslose gemeinsame Nutzung von Dateisystemen durch NFS gewährleisten, sind jedoch auch die Ursache für Sicherheitsprobleme. In der Vergangenheit wurden für die meisten NFS-Implementierungen die UNIX-Authentifizierung (oder AUTH_SYS) verwendet, während bessere Authentifizierungsverfahren wie beispielsweise AUTH_DH bereits zur Verfügung standen. Bei Verwendung der UNIX-Authentifizierung authentifiziert ein NFS-Server eine

Dateianforderung, indem anstelle des Benutzers der Computer authentifiziert wird, von dem die Anforderung ausgeht. Dadurch kann ein Clientbenutzer den Befehl `su` ausführen und der Eigentümer einer Datei sein. Wenn die DH-Authentifizierung verwendet wird, authentifiziert der NFS-Server den Benutzer, wodurch diese Art der Imitation bedeutend erschwert wird.

Jeder, der Root-Zugriff hat und über Kenntnisse über Netzwerkprogrammierung verfügt, kann Daten in das Netzwerk einschleusen oder diese aus dem Netzwerk extrahieren. Die größte Gefahr stellen Angriffe dar, bei denen Daten eingeschleust werden. Durch Generierung der richtigen Pakete oder durch Aufzeichnung von Dialogen, die später wiedergegeben werden, kann beispielsweise ein Benutzer imitiert werden. Diese Angriffe gefährden die Datenintegrität. Angriffe durch passives Mithören, bei dem nur das Netzwerk abgehört wird, ohne eine Person zu imitieren, sind weniger gefährlich, da die Datenintegrität nicht gefährdet wird. Benutzer können vertrauliche Daten schützen, indem sie die Daten verschlüsseln, die über das Netzwerk gesendet werden.

Ein allgemeiner Ansatz zur Behebung von Netzwerksicherheitsproblemen besteht darin, entsprechende Lösungen in den einzelnen Anwendungen zu implementieren. Ein besserer Ansatz besteht darin, ein standardmäßiges Authentifizierungssystem für alle Anwendungen zu installieren.

Das Betriebssystem Solaris bietet ein Authentifizierungsystem auf der Ebene des RPC (Remote Procedure Call). RPC ist ein Mechanismus, auf dem der NFS-Vorgang basiert. Dieses System, das als sicheres RPC bezeichnet wird, verbessert spürbar die Sicherheit von Netzwerkumgebungen und bietet Services wie beispielsweise dem NFS-System mehr Sicherheit. Da das NFS-System die vom sicheren RPC bereitgestellten Funktionen verwendet, wird es in diesem Zusammenhang auch als sicheres NFS-System bezeichnet.

Secure RPC

Sicheres RPC ist eine wichtige Grundlage für den Einsatz des sicheren NFS-Systems. Das Ziel vom sicheren RPC ist die Einrichtung eines Systems, das mindestens so sicher wie ein Teilnehmersystem ist. In einem Teilnehmersystem verwenden alle Benutzer einen einzelnen Computer. Jeder Benutzer wird durch ein Anmeldepasswort authentifiziert. Mit der DES-Authentifizierung (Data Encryption Standard) wird derselbe Authentifizierungsprozess durchgeführt. Die Benutzer können sich bei jedem Remote-Computer wie bei einem lokalen Terminal anmelden. Die Anmeldepasswörter der Benutzer gewährleisten die Netzwerksicherheit. In einem Teilnehmersystem darf der Systemadministrator aus ethischen Gründen kein Passwort ändern, um einen Benutzer zu imitieren. Im sicheren RPC wird dem Netzwerkadministrator vertraut und vorausgesetzt, dass keine Einträge in einer Datenbank geändert werden, in der der *öffentliche Schlüssel* gespeichert sind.

Um ein RPC-Authentifizierungssystem zu verstehen, müssen Sie zwei Begriffe kennen: Berechtigungsnachweise und Nachweise. Beispielsweise dienen Berechtigungsnachweise in

Verbindung mit Ausweisen zur Identifizierung einer Person: Name, Adresse und Geburtsdatum. Der Nachweis ist das Foto, das zum Ausweis gehört. Ob der Ausweis gestolen ist oder der Person gehört, die im Besitz des Ausweises ist, lässt sich feststellen, indem das Ausweisfoto mit der Person verglichen wird. In RPC sendet der Clientprozess zusammen mit jeder RPC-Anforderung sowohl Berechtigungsnachweise als auch einen Nachweis an den Server. Der Server sendet nur einen Nachweis zurück, da der Client die Berechtigungsnachweise des Servers bereits "kennt".

Die RPC-Authentifizierung ist unbegrenzt erweiterungsfähig, es können demnach zahlreiche Authentifizierungssysteme wie beispielsweise UNIX, DH oder KERB integriert werden.

Wenn die UNIX-Authentifizierung von einem Netzwerkdienst verwendet wird, ist in den Berechtigungsnachweisen der Hostname des Clients, die UID, die GID und die Gruppenzugriffsliste enthalten. Im Nachweis ist jedoch nichts enthalten. Da also kein Nachweis vorhanden ist, könnte ein Superuser Berechtigungsnachweise fälschen, indem er einen Befehl wie beispielsweise `su` verwendet. Ein weiteres Problem im Zusammenhang mit der UNIX-Authentifizierung besteht darin, dass bei der UNIX-Authentifizierung vorausgesetzt wird, dass alle Computer in einem Netzwerk UNIX-Computer sind. Die UNIX-Authentifizierung schlägt fehl, wenn sie bei anderen Betriebssystemen in einem heterogenen Netzwerk angewendet wird.

Um die mit der UNIX-Authentifizierung verbundenen Probleme zu vermeiden, wird im sicheren RPC die DH-Authentifizierung verwendet.

DH-Authentifizierung

Bei der DH-Authentifizierung werden der DES (Data Encryption Standard) und Diffie-Hellman-Verschlüsselung mit öffentlichen Schlüsseln verwendet, um Benutzer und Computer in einem Netzwerk zu authentifizieren. DES ist ein standardmäßiger Verschlüsselungsmechanismus. Diffie-Hellman-Verschlüsselung mit öffentlichem Schlüssel ist ein Ziffernsystem, das zwei Schlüssel umfasst: einen öffentlichen und einen geheimen Schlüssel. Die öffentlichen und die geheimen Schlüssel werden im Namespace gespeichert. NIS speichert die Schlüssel in der Map für öffentliche Schlüssel. Diese Maps enthalten die öffentlichen und geheimen Schlüssel für alle potentiellen Benutzer. Weitere Informationen zum Einrichten dieser Tabellen finden Sie unter *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*.

Die Sicherheit der DH-Authentifizierung basiert auf der Fähigkeit eines Absenders, die aktuelle Zeit zu verschlüsseln, die dann vom Empfänger entschlüsselt und mit der eigenen Zeit verglichen wird. Der Zeitstempel wird mit DES verschlüsselt. Damit dieses Schema funktioniert, müssen folgende Voraussetzungen erfüllt sein:

- Die beiden Agenten müssen die aktuelle Zeit vereinbaren.
- Der Absender und der Empfänger müssen den gleichen Verschlüsselungsschlüsseln verwenden.

Wenn ein Netzwerk ein Zeitsynchronisierungsprogramm ausführt, wird die Zeit auf dem Client und dem Server automatisch synchronisiert. Wenn kein Zeitsynchronisierungsprogramm zur Verfügung steht, können die Zeitstempel berechnet werden, indem die Zeit des Servers anstelle der Netzwerkzeit verwendet wird. Der Client fragt beim Server die Zeit ab, bevor er mit der RPC-Sitzung beginnt. Dann berechnet er die Zeitdifferenz zwischen seiner eigenen Uhr und der des Servers. Diese Differenz wird verwendet, um die Uhr des Clients anzupassen, wenn die Zeitstempel berechnet werden. Wenn die Uhren des Clients und des Servers nicht mehr synchron laufen, lehnt der Server die Anforderungen des Clients ab. Das auf dem Server ausgeführte DH-Authentifizierungssystem führt erneut eine Synchronisierung mit dem Server durch.

Der Client und der Server erhalten den gleichen Verschlüsselungsschlüssel, indem ein zufälliger *Dialogschlüssel* generiert wird, der auch als *Sitzungsschlüssel* bezeichnet wird, und indem die Verschlüsselung mit öffentlichen Schlüsseln verwendet wird, um einen *allgemeinen Schlüssel* abzuleiten. Der allgemeine Schlüssel ist ein Schlüssel, den nur der Client und der Server ableiten können. Der Dialogschlüssel wird verwendet, um den Zeitstempel des Clients zu verschlüsseln und zu entschlüsseln. Der allgemeine Schlüssel wird verwendet, um den Dialogschlüssel zu verschlüsseln und zu entschlüsseln.

KERB-Authentifizierung

Kerberos ist ein Authentifizierungssystem, das am MIT entwickelt wurde. Kerberos bietet zahlreiche Verschlüsselungstypen, darunter DES. Kerberos-Unterstützung wird nicht mehr als Teil von Secure RPC bereitgestellt, aber Solaris enthält eine serverseitige und clientseitige Implementierung. Weitere Informationen zur Implementierung der Kerberos-Authentifizierung finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Verwenden vom sicheren RPC mit NFS

Wenn Sie vorhaben, das sichere RPC zu verwenden, sollten Sie Folgendes berücksichtigen:

- Wenn ein Server abstürzt, wenn niemand in der Nähe ist (beispielsweise nach einem Stromausfall), werden alle geheimen Schlüssel gelöscht, die im System gespeichert sind. Dann kann kein Prozess auf sichere Netzwerkdienste zugreifen oder ein NFS-Dateisystem einhängen. Die wichtigen Prozesse während eines Neustarts werden normalerweise als `root` ausgeführt. Darum würden diese Prozesse funktionieren, wenn der geheime Schlüssel des Root-Benutzers gespeichert wäre. Allerdings kennt niemand das Passwort, das zum Entschlüsseln des Schlüssels benötigt wird. `keylogin -r` erlaubt `root`, den unverschlüsselten geheimen Schlüssel in der Datei `/etc/.rootkey` zu speichern, die von `keyserv` gelesen wird.
- Manche Systeme werden mithilfe einer Root-Anmelde-Shell auf der Konsole und ohne Aufforderung zur Eingabe eines Passworts im Einzelbenutzermodus neu gestartet. In solchen Fällen ist die physische Sicherheit von vorrangiger Bedeutung.

- Das Booten von Computern ohne lokalen Massenspeicher ist nicht umfassend sicher. Der Boot-Server könnte imitiert werden, um einen falschen Kernel zu booten, mit dem beispielsweise ein Datensatz Ihres geheimen Schlüssels auf einem Remote-Computer erstellt wird. Das sichere NFS-System bietet nur dann Schutz, wenn der Kernel und der Schlüsselserver ausgeführt werden. Ansonsten gibt es keine Möglichkeit, die Replikationen zu authentifizieren, die vom Boot-Server bereitgestellt werden. Diese Beschränkung kann ein schwerwiegendes Problem sein, erfordert aber einen ausgeklügelten Angriff unter Verwendung des Kernel-Quellcodes. Beim kriminellen Vorgehen werden auf jeden Fall Spuren hinterlassen. Wenn Sie im Netzwerk nach Boot-Servern suchen, würden Sie den falschen Standort des Boot-Servers finden.
- Die meisten setuid-Programme sind im Besitz des `root`-Benutzers. Wenn der geheime Schlüssel für `root` in `/etc/.rootkey` gespeichert wird, verhalten sich diese Programme wie gewöhnlich. Wenn ein setuid-Programm jedoch im Besitz eines Benutzers ist, funktioniert es eventuell nicht immer richtig. Ein setuid-Programm ist beispielsweise im Besitz von `dave` und `dave` hat sich nach dem Booten nicht beim Computer angemeldet. Das Programm würde dann nicht auf die sicheren Netzwerkdienste zugreifen können.
- Wenn Sie sich (mithilfe von `login` , `rlogin` oder `telnet`) bei einem Remote-Computer anmelden und `keylogin` verwenden, um Zugriff zu erhalten, geben Sie den Zugriff auf Ihr Konto frei. Der Grund dafür ist der, dass Ihr geheimer Schlüssel an den Schlüsselserver des Computers weitergegeben wird, auf dem Ihr geheimer Schlüssel dann gespeichert wird. Dieser Prozess ist nur dann von Bedeutung, wenn Sie den Remote-Computer nicht als vertrauenswürdig betrachten. Wenn Sie jedoch Zweifel haben, melden Sie sich nicht bei dem Remote-Computer an, wenn dieser ein Passwort verlangt. Verwenden Sie stattdessen die NFS-Umgebung, um Dateisysteme einzuhängen, die vom Remote-Computer gemeinsam genutzt werden. Als Alternative können Sie `keylogout` verwenden, um den geheimen Schlüssel auf dem Schlüsselserver zu löschen.
- Wenn ein Home-Verzeichnis mit der Option `-o sec=dh` zur gemeinsamen Nutzung freigegeben wird, können Remote-Anmeldungen ein Problem darstellen. Wenn die `/etc/hosts.equiv`- oder `~/.rhosts`-Datei nicht so eingerichtet ist, dass ein Passwort angefordert wird, kann die Anmeldung erfolgreich durchgeführt werden. Die Benutzer können jedoch nicht auf ihre Home-Verzeichnisse zugreifen, weil die Authentifizierung lokal durchgeführt wurde. Wenn ein Benutzer zur Eingabe eines Passworts aufgefordert wird, kann der Benutzer auf sein Home-Verzeichnis zugreifen, wenn das Passwort mit dem Netzwerkpasswort übereinstimmt.

Autofs-Maps

Autofs verwendet drei Arten von Maps:

- Master-Map
- Direkte Maps
- Indirekte Maps

Master-Autofs-Maps

Die `auto_master`-Map dient zur Zuordnung eines Verzeichnisses zu einer Map. Die Map ist eine Hauptliste, in der alle Maps angegeben sind, die von autofs geprüft werden. Das folgende Beispiel zeigt, was in einer `auto_master`-Datei enthalten sein kann.

BEISPIEL 6–3 `/etc/auto_master`-Beispieldatei

```
# Master map for automounter
#
+auto_master
/net            -hosts           -nosuid,nobrowse
/home           auto_home        -nobrowse
/-              auto_direct     -ro
```

In diesem Beispiel wird die generische `auto_master`-Datei mit einem Zusatz für die `auto_direct`-Map dargestellt. Jede Zeile in der Master-Map `/etc/auto_master` hat folgende Syntax:

mount-point map-name [*mount-options*]

mount-point — *mount-point* ist der vollständige (absolute) Pfadname eines Verzeichnisses. Wenn das Verzeichnis nicht vorhanden ist, wird das Verzeichnis von autofs erstellt, sofern dies möglich ist. Ist ein Verzeichnis vorhanden, das nicht leer ist, und wird ein Objekt in das Verzeichnis eingehängt, wird der Inhalt des Verzeichnisses ausgeblendet. In solch einem Fall gibt autofs eine Warnung aus.

Wenn ein Einhängepunkt mit `/-` angegeben wird, bedeutet das, dass die betreffende Map eine direkte Map ist. Eine solche Schreibweise weist auch darauf hin, dass kein bestimmter Einhängepunkt der Map zugeordnet ist.

map-name — *map-name* ist die Map, die von autofs verwendet wird, um nach Verweisen auf Speicherorte oder nach Einhängeinformationen zu suchen. Wenn dem Namen ein Schrägstrich (/) vorangestellt ist, interpretiert autofs den Namen als lokale Datei. Anderenfalls sucht autofs mithilfe des Suchvorgangs, der in der Name Service Switch-Konfigurationsdatei (`/etc/nsswitch.conf`) angegeben ist, nach den Einhängeinformationen. Spezielle Maps werden auch für `/net` verwendet. Weitere Informationen finden Sie unter „Einhängepunkt `/net`“ auf Seite 214.

mount-options — *mount-points* ist eine optionale, durch Komma getrennte Liste von Optionen für das Einhängen von Objekten, die im Map-Namen angegeben sind, es sei denn, in den Einträgen in der Liste der Map-Namen sind andere Optionen aufgeführt. Optionen für jeden Dateisystemtyp sind auf der entsprechenden Manpage aufgelistet. Die NFS-spezifische Einhängeoptionen finden Sie beispielsweise auf der Manpage

`mount_nfs(1M)`. Die Optionen `bg` (Hintergrund) und `fg` (Vordergrund) haben für NFS-spezifische Einhängepunkte keine Gültigkeit.

Eine Zeile, die mit dem Nummernzeichen (#) beginnt, ist ein Kommentar. Der gesamte bis zum Ende der Zeile nachfolgende Text wird ignoriert.

Um lange Zeilen in kürzere Zeilen aufzuteilen, setzen Sie einen umgekehrten Schrägstrich (\) an das Ende der Zeile. Ein Eintrag kann maximal 2024 Zeichen haben.

Hinweis – Wenn für zwei Einträge der gleiche Einhängepunkt verwendet wird, wird der erste Eintrag vom Befehl `automount` verwendet. Der zweite Eintrag wird ignoriert.

Einhängepunkt `/home`

Der Einhängepunkt `/home` ist das Verzeichnis, unter dem die Objekte der Einträge eingehängt werden, die in `/etc/auto_home` (eine indirekte Map) aufgelistet sind.

Hinweis – Autofs wird auf allen Computern ausgeführt und unterstützt standardmäßig `/net` und `/home` (automatisch eingehängte Verzeichnisse). Diese Standardeinstellungen können durch die Einträge in der `auto.master` -NIS-Map oder in der `auto_master`-NIS+-Map oder durch lokales Bearbeiten der `/etc/auto_master`-Datei außer Kraft gesetzt werden.

Einhängepunkt `/net`

Autofs hängt unter dem Verzeichnis `/net` alle Objekte der Einträge in der speziellen Map `-hosts` ein. Die Map ist eine integrierte Map, die nur die Hosts-Datenbank verwendet. Angenommen, der Computer `gumbo` ist in der Hosts-Datenbank enthalten und exportiert eines seiner Dateisysteme. Durch den folgenden Befehl wird das aktuelle Verzeichnis in das Root-Verzeichnis des Computers `gumbo` geändert.

```
% cd /net/gumbo
```

Autofs kann nur die *exportierten* Dateisysteme des Hosts `gumbo` einhängen, d. h. die Dateisysteme auf einem Server, die für Netzwerkbenutzer zur Verfügung stehen, nicht aber die Dateisysteme auf einer lokalen Festplatte. Darum kann auf die Dateien und Verzeichnisse auf `gumbo` eventuell nicht über `/net/gumbo` zugegriffen werden.

Bei Verwendung der `/net`-Zugriffmethode ist der Servername im Pfad enthalten und damit speicherortabhängig. Wenn Sie vorhaben, ein exportiertes Dateisystem von einem Server auf einen anderen umzusetzen, kann es sein, dass der Pfad nicht mehr funktioniert. Anstatt `/net` zu verwenden, sollten Sie einen Eintrag in eine Map einfügen, der für das gewünschte Dateisystem bestimmt ist.

Hinweis – Autofs prüft die Exportliste des Servers nur während der Einhängung. Nachdem die Dateisysteme eines Servers eingehängt wurden, setzt sich autofs erst dann wieder mit dem Server in Verbindung, wenn die Dateisysteme des Servers automatisch ausgehängt werden. Aus diesem Grund werden neu exportierte Dateisysteme erst dann erkannt, wenn Dateisysteme auf dem Client nach dem Aushängen wieder eingehängt sind.

Direkte Autofs-Map

Eine direkte Map ist ein automount-Punkt. Bei einer direkten Map besteht eine direkte Verbindung zwischen einem Einhängepunkt auf dem Client und einem Verzeichnis auf dem Server. Direkte Maps haben einen vollständigen Pfadnamen und geben die Beziehung explizit an. Es folgt eine typische `/etc/auto_direct` -Map:

```
/usr/local          -ro \
   /bin                   ivy:/export/local/sun4 \
   /share                 ivy:/export/local/share \
   /src                   ivy:/export/local/src
/usr/man            -ro    oak:/usr/man \
                           rose:/usr/man \
                           willow:/usr/man
/usr/games          -ro    peach:/usr/games
/usr/spool/news     -ro    pine:/usr/spool/news \
                           willow:/var/spool/news
```

Zeilen in direkten Maps haben folgende Syntax:

key [*mount-options*] *location*

key — *key* ist der Pfadname des Einhängepunkts in einer direkten Map.

mount-options — *mount-options* sind die Optionen, die für die betreffende Einhängung gelten sollen. Die Optionen sind nur dann erforderlich, wenn die Optionen sich von den standardmäßigen Zuordnungswerten unterscheiden. Optionen für jeden Dateisystemtyp sind auf der entsprechenden Manpage aufgelistet. NFS-spezifische Einhängeoptionen finden Sie beispielsweise auf der Manpage `mount_nfs(1M)`.

location — *location* ist der Speicherort des Dateisystems. Eines oder mehrere Dateisysteme werden mit *server*: *pathname* für NFS-Dateisysteme oder :*devicename* für High Sierra-Dateisysteme (HSFS) angegeben.

Hinweis – Der *pathname* sollte keinen Einhängepunkt enthalten, an dem eine automatische Einhängung stattgefunden hat. Der *pathname* sollte der aktuelle absolute Pfad zum Dateisystem sein. Beispielsweise sollte der Speicherort eines Home-Verzeichnisses mit *server*`:/export/home/`*username* angegeben werden, nicht mit *server* `:/home/`*username*.

Eine Zeile, die mit dem Nummernzeichen (#) beginnt, ist wie in der Master-Map ein Kommentar. Der gesamte bis zum Ende der Zeile nachfolgende Text wird ignoriert. Setzen Sie einen umgekehrten Schrägstrich an das Ende der Zeile, um lange Zeilen in kürzere aufzuteilen.

Von allen Maps sind die Einträge in einer direkten Map den entsprechenden Einträgen in `/etc/vfstab` am ähnlichsten. Ein Eintrag in `/etc/vfstab` kann wie folgt aussehen:

```
dancer:/usr/local - /usr/local/tmp nfs - yes ro
```

Der äquivalente Eintrag in einer direkten Map sieht wie folgt aus:

```
/usr/local/tmp     -ro     dancer:/usr/local
```

Hinweis – Zwischen den Automounter-Maps findet keine Verkettung von Optionen statt. Durch Optionen, die in eine Automounter-Maps eingefügt werden, werden alle Optionen außer Kraft gesetzt, die in zuvor durchsuchten Maps aufgelistet sind. Beispielsweise werden die in der `auto_master`-Map enthaltenen Optionen durch die entsprechenden Einträge in einer anderen Map außer Kraft gesetzt.

Weitere wichtige Funktionen, die mit dieser Map in Zusammenhang stehen, finden Sie unter „Wie autofs die nächsten schreibgeschützten Dateien für Clients auswählt (mehrere Speicherorte)“ auf Seite 223.

Einhängepunkt `/-`

Der in Beispiel 6–3 angegebene Einhängepunkt `/-` zeigt autofs an, die Einträge in `auto_direct` keinen speziellen Einhängepunkten zuzuordnen. Indirekte Maps verwenden Einhängepunkte, die in der `auto_master`-Datei definiert sind. Direkte Maps verwenden Einhängepunkte, die in der angegebenen Map definiert sind. Bitte beachten Sie: In einer direkten Map ist der Schlüssel oder der Einhängepunkt ein vollständiger Pfadname.

Eine NIS- oder NIS+-`auto_master`-Datei kann nur einen direkten Map-Eintrag haben, weil der Einhängepunkt ein eindeutiger Wert im Namespace sein muss. Eine `auto_master`-Datei, die eine lokale Datei ist, kann eine beliebige Anzahl von direkten Map-Einträgen haben, wenn es sich nicht um duplizierte Einträge handelt.

Indirekte autofs-Maps

Eine indirekte Map verwendet einen Ersatzwert eines Schlüssels, um die Beziehung zwischen einem Einhängepunkt auf dem Client und einem Verzeichnis auf dem Server herzustellen. Indirekte Maps dienen dazu, um auf spezifische Dateisysteme wie beispielsweise Home-Verzeichnisse zuzugreifen. Die `auto_home`-Map ist eine Beispiel für eine indirekte Map.

Zeilen in indirekten Maps haben folgende Syntax:

key [*mount-options*] *location*

key — *key* ist ein einfacher Name in einer indirekten Map, der keine Schrägstriche aufweist.

mount-options — *mount-options* sind die Optionen, die für die betreffende Einhängung gelten sollen. Die Optionen sind nur dann erforderlich, wenn die Optionen sich von den standardmäßigen Zuordnungswerten unterscheiden. Optionen für jeden Dateisystemtyp sind auf der entsprechenden Manpage aufgelistet. Die NFS-spezifische Einhängeoptionen finden Sie beispielsweise auf der Manpage `mount_nfs(1M)`.

location — *location* ist der Speicherort des Dateisystems. Eines oder mehrere Dateisysteme werden mit *server*: *pathname* angegeben.

Hinweis – Der *pathname* sollte keinen Einhängepunkt enthalten, an dem eine automatische Einhängung stattgefunden hat. Der *pathname* sollte der aktuelle absolute Pfad zum Dateisystem sein. Der Speicherort eines Verzeichnisses beispielsweise sollte mit *server*`:/usr/local` angegeben werden, nicht mit *server*`:/net/` *server*`/usr/local`.

Eine Zeile, die mit dem Nummernzeichen (#) beginnt, ist wie in der Master-Map ein Kommentar. Der gesamte bis zum Ende der Zeile nachfolgende Text wird ignoriert. Setzen Sie einen umgekehrten Schrägstrich (\) an das Ende der Zeile, um lange Zeilen in kürzere aufzuteilen. Beispiel 6–3 zeigt eine `auto_master`-Map, die den folgenden Eintrag enthält:

```
/home      auto_home        -nobrowse
```

`auto_home` ist der Name der indirekten Map, in der die Einträge der Objekte enthalten sind, die unter `/home` eingehängt werden sollen. Eine typische `auto_home`-Map kann Folgendes enthalten:

```
david                 willow:/export/home/david
rob                   cypress:/export/home/rob
gordon                poplar:/export/home/gordon
rajan                 pine:/export/home/rajan
tammy                 apple:/export/home/tammy
```

```
jim                     ivy:/export/home/jim
linda    -rw,nosuid     peach:/export/home/linda
```

Die vorherige Map befindet sich beispielsweise auf Host `oak`. Angenommen, für den Benutzer `linda` ist ein Eintrag in der Passwortdatenbank enthalten, der das Home-Verzeichnis des Benutzers mit `/home/linda` angibt. Wenn sich `linda` beim Computer `oak` anmeldet, hängt autofs das Verzeichnis `/export/home/linda` ein, das sich auf dem Computer `peach` befindet. Das Home-Verzeichnis des Benutzers wird mit Lese- und Schreibzugriff und unter Verwendung der Option nosuid eingehängt.

Angenommen, Folgendes trifft zu: Das Home-Verzeichnis des Benutzers linda wird in der Passwortdatenbank mit `/home/linda` angegeben. Jeder Benutzer, einschließlich linda, kann auf diesen Pfad von jedem Computer aus zugreifen, der mithilfe der Master-Map eingerichtet wurde, die auf die im vorangegangenen Beispiel genannte Map verweist.

Unter diesen Voraussetzungen kann der Benutzer linda den Befehl `login` oder den Befehl `rlogin` auf jedem dieser Computer ausführen und sein Home-Verzeichnis einhängen.

Jetzt kann der Benutzer linda auch den folgenden Befehl eingeben:

```
% cd ~david
```

Autofs hängt das Home-Verzeichnis des Benutzers david für den Benutzer linda ein (sofern dies gemäß allen Berechtigungen zulässig ist).

Hinweis – Zwischen den Automounter-Maps findet keine Verkettung von Optionen statt. Durch Optionen, die in eine Automounter-Map eingefügt werden, werden alle Optionen außer Kraft gesetzt, die in zuvor durchsuchten Maps aufgelistet sind. Die in der `auto_master`-Map enthaltenen Optionen werden beispielsweise durch die entsprechenden Einträge in einer anderen Map außer Kraft gesetzt.

In einem Netzwerk ohne Name Service müssen Sie alle relevanten Dateien (wie beispielsweise `/etc/passwd`) auf allen Systemen im Netzwerk ändern, um dem Benutzer linda den Zugriff auf seine Dateien zu ermöglichen. Bei NIS nehmen Sie die Änderungen am NIS-Master-Server vor und geben die relevanten Datenbanken an die Slave-Server weiter. In einem Netzwerk, in dem NIS+ ausgeführt wird, erfolgt die Weitergabe der relevanten Datenbanken an die Slave-Server automatisch, nachdem die Änderungen vorgenommen wurden.

Funktionsweise von autofs

Autofs ist ein clientseitiger Service, der zum automatischen Einhängen von Dateisystemen dient. Es folgen die Komponenten, die beim automatischen Einhängen zusammenwirken:

- `automount`-Befehl
- `autofs`-Dateisystem
- `automountd`-Dämon

Der automount-Service, `svc:/system/filesystem/autofs` , der während des Systemstarts aufgerufen wird, liest die Master-Map-Datei `auto_master`, um eine anfängliche Gruppe von autofs-Einhängungen zu erstellen. Diese autofs-Einhängungen werden beim Start nicht automatisch eingehängt. Vielmehr sind diese Einhängungen Punkte, unter denen Dateisysteme zu späteren Zeitpunkten eingehängt werden. Diese Punkte werden auch als Aktivierungsknoten bezeichnet.

Nachdem die autofs-Einhängungen eingerichtet wurden, können unter diesen Einhängungen weitere Dateisysteme eingehängt werden. Wenn autofs beispielsweise eine Anforderung zum Zugriff auf ein Dateisystem erhält, das derzeit nicht eingehängt ist, ruft autofs den Dämon `automountd` auf, der dann das betreffende Dateisystem einhängt.

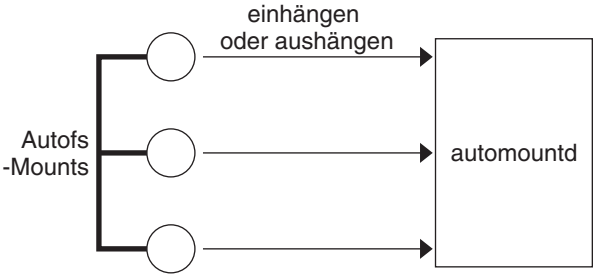
Nach dem anfänglichen Einhängen der autofs-Einhängepunkte wird der Befehl `automount` verwendet, um die autofs-Einhängepunkte nach Bedarf zu aktualisieren. Mithilfe des Befehls wird die Liste der Einhängungen in der `auto_master`-Map mit der Liste der eingehängten Dateisysteme in der Einhängetabellendatei `/etc/mnttab` (vormals `/etc/mtab`) verglichen. `automount` nimmt dann die entsprechenden Änderungen vor. Dieser Vorgang erlaubt Systemadministratoren, Einhängeinformationen in `auto_master` zu ändern und diese Änderungen in autofs-Vorgängen verwenden zu lassen, ohne den autofs-Dämon zu stoppen und neu zu starten. Nachdem das Dateisystem eingehängt wurde, ist beim zweiten Zugriff erst dann ein Eingreifen von `automountd` erforderlich, wenn das Dateisystem automatisch ausgehängt wurde.

Im Gegensatz zum Befehl `mount` liest `automount` nicht die `/etc/vfstab`-Datei (die sich auf die einzelnen Computer bezieht), damit aufgelistete Dateisysteme eingehängt werden können. Der Befehl `automount` wird durch den Namespace oder lokale Dateien innerhalb einer Domain und auf Computern gesteuert.

Es folgt eine vereinfachte Beschreibung der Funktionsweise von autofs.

Der automount-Dämon `automountd` wird während des Boot-Vorgangs durch den Service `svc:/system/filesystem/autofs` gestartet. Siehe dazu Abbildung 6–3. Dieser Service führt auch den Befehl `automount` aus, der die Master-Map liest und die autofs-Einhängepunkte installiert. Weitere Informationen finden Sie unter „Wie autofs den Navigationprozess startet (Master-Map)“ auf Seite 221.

ABBILDUNG 6–3 Der `svc:/system/filesystem/autofs`-Service startet `automount`.



Autofs ist ein Kernel-Dateisystem zur Unterstützung des automatischen Ein- und Aushängens.

Wenn eine Anforderung gesendet wird, um auf ein Dateisystem an einem autofs-Einhängepunkt zuzugreifen, geschieht Folgendes:

1. Autofs fängt die Anforderung ab.
2. Autofs sendet eine Meldung an `automountd`, damit das betreffende Dateisystem ausgehängt wird.
3. `automountd` lokalisiert die Dateisysteminformationen in einer Map, erstellt die Aktivierungsknoten und führt die Einhängung aus.
4. Autofs lässt die weitere Verarbeitung der abgefangenen Anforderung zu.
5. Nach einer bestimmten Zeit der Inaktivität hängt autofs das Dateisystem aus.

Hinweis – Einhängungen, die durch den autofs-Service gesteuert werden, sollten nicht manuell ein- oder ausgehängt werden. Selbst wenn dies erfolgreich durchgeführt werden kann, wird nicht vom autofs-Service geprüft, ob das betreffende Objekt ausgehängt wurde, woraus Inkonsistenzen resultieren können. Durch einen Neustart werden alle autofs-Einhängepunkte entfernt.

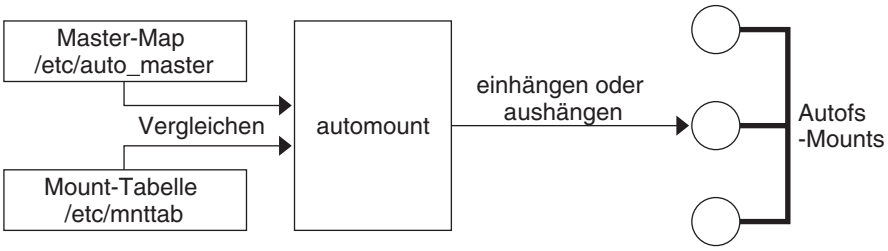
Wie autofs durch das Netzwerk navigiert (Maps)

Autofs durchsucht eine Reihe von Maps, um durch das Netzwerk zu navigieren. Maps sind Dateien, die Informationen wie beispielsweise die Passworteinträge aller Benutzer in einem Netzwerk oder die Namen aller Hostcomputer in einem Netzwerk enthalten. Die Maps enthalten netzwerkübergreifende Entsprechungen der UNIX-Administrationsdateien. Maps sind lokal oder über einen Netzwerk-Name Service wie NIS oder NIS+ verfügbar. Lesen Sie dazu „Modifizieren, wie autofs im Netzwerk navigiert (Modifizieren von Maps)“ auf Seite 230.

Wie autofs den Navigationprozess startet (Master-Map)

Mit dem Befehl `automount` wird die Master-Map beim Systemstart gelesen. Jeder Eintrag in der Master-Map ist der Name einer direkten oder indirekten Map, eines Pfads oder von Einhängeoptionen (siehe Abbildung 6–4). Die Reihenfolge der Einträge ist nicht von Bedeutung. `automount` vergleicht die Einträge in der Master-Map mit den Einträgen in der Einhängetabelle, um eine aktuelle Liste zu erstellen.

ABBILDUNG 6–4 Navigation durch die Master-Map



Autofs-Einhängeprozess

Wie der autofs-Service reagiert, wenn eine Einhängungsanforderung ausgelöst wird, hängt davon ab, wie die Automounter-Maps konfiguriert sind. Der Einhängeprozess ist in der Regel für alle Einhängepunkte der gleiche. Jedoch ändert sich das Endergebnis in Abhängigkeit vom angegebenen Einhängepunkt und von der Komplexität der Maps. Der Einhängevorgang umfasst die Erstellung von Aktivierungsknoten.

Einfache autofs-Einhängung

Zur Veranschaulichung des autofs-Einhängeprozesses wird angenommen, dass die folgenden Dateien installiert sind.

```
$ cat /etc/auto_master
# Master map for automounter
#
+auto_master
/net        -hosts        -nosuid,nobrowse
/home       auto_home     -nobrowse
/share      auto_share
$ cat /etc/auto_share
# share directory map for automounter
#
ws          gumbo:/export/share/ws
```

Wenn auf das /share-Verzeichnis zugegriffen wird, erstellt der autofs-Service einen Aktivierungsknoten für /share/ws, ein Eintrag in /etc/mnttab, der wie folgt aussehen kann:

```
-hosts  /share/ws     autofs  nosuid,nobrowse,ignore,nest,dev=###
```

Wenn auf das /share/ws-Verzeichnis zugegriffen wird, führt der autofs-Service folgende Schritte aus, um den Prozess durchzuführen:

1. Prüfung der Verfügbarkeit des Einhängeservice des Servers
2. Einhängen des angeforderten Dateisystems unter /share. Jetzt enthält die /etc/mnttab-Datei die folgenden Einträge:

   ```
   -hosts  /share/ws     autofs  nosuid,nobrowse,ignore,nest,dev=###
   gumbo:/export/share/ws /share/ws   nfs   nosuid,dev=####    #####
   ```

Hierarchisches Einhängen

Wenn in den Automounter-Dateien mehrere Schichten definiert sind, wird der Einhängeprozess komplexer. Angenommen, Sie fügen Folgendes in die /etc/auto_shared -Datei aus dem vorangegangenen Beispiel ein:

```
# share directory map for automounter
#
ws       /       gumbo:/export/share/ws
         /usr    gumbo:/export/share/ws/usr
```

Der Einhängeprozess ist im Wesentlichen derselbe wie im vorangegangenen Beispiel, wenn auf den /share/ws-Einhängepunkt zugegriffen wird. Außerdem wird ein Aktivierungsknoten für die nächste Ebene (/usr) im /share/ws-Dateisystem erstellt, sodass die nächste Ebene eingehängt werden kann, wenn auf sie zugegriffen wird. In diesem Beispiel muss /export/share/ws/usr auf dem NFS-Server vorhanden sein, damit der Aktivierungsknoten erstellt werden kann.

Achtung – Verwenden Sie nicht die Option -soft, wenn Sie hierarchische Ebenen angeben. Eine Erläuterung dieser Beschränkung finden Sie unter „Autofs-Aushängung“ auf Seite 222.

Autofs-Aushängung

Das Aushängen nach einer bestimmten Leerlaufzeit wird von unten nach oben durchgeführt (in umgekehrter Reihenfolge des Einhängens). Wenn eines der Verzeichnisse auf einer höheren Ebene der Hierarchie verwendet wird, werden nur die Dateisysteme unter dem betreffenden Verzeichnis ausgehängt. Während des Aushängeprozesses werden Aktivierungsknoten entfernt, wonach das Dateisystem ausgehängt wird. Wenn das Dateisystem beschäftigt ist, schlägt das Aushängen fehl und die Aktivierungsknoten werden erneut installiert.

Achtung – Verwenden Sie nicht die Option `-soft`, wenn Sie hierarchische Ebenen angeben. Wenn die Option `-soft` verwendet wird, können Anforderungen zur erneuten Installation der Aktivierungsknoten eine Zeitüberschreitung auslösen. Wenn die Aktivierungsknoten nicht installiert werden können, ist kein Zugriff auf die nächste Ebene der Einhängungen möglich. Die einzige Möglichkeit, dieses Problem zu beheben, besteht darin, alle Komponenten in der Hierarchie vom Automounter aushängen zu lassen. Der Automounter kann das Aushängen durchführen, indem er entweder darauf wartet, dass die Dateisysteme automatisch ausgehängt werden, oder indem er das System neu startet.

Wie autofs die nächsten schreibgeschützten Dateien für Clients auswählt (mehrere Speicherorte)

Die direkte Beispiel-Map enthält Folgendes:

```
/usr/local          -ro \
   /bin                   ivy:/export/local/sun4\
   /share                 ivy:/export/local/share\
   /src                   ivy:/export/local/src
/usr/man            -ro    oak:/usr/man \
                           rose:/usr/man \
                           willow:/usr/man
/usr/games          -ro    peach:/usr/games
/usr/spool/news     -ro    pine:/usr/spool/news \
                           willow:/var/spool/news
```

Die Einhängepunkte `/usr/man` und `/usr/spool/news` listen mehrere Speicherorte auf: drei für den ersten Einhängepunkt und zwei für den zweiten Einhängepunkt. Jeder der replizierten Speicherorte kann denselben Service für jeden Benutzer bereitstellen. Dieses Verfahren ist nur dann fehleranfällig, wenn Sie ein schreibgeschütztes Dateisystem einhängen, da Sie die Kontrolle über die Speicherorte der Dateien haben müssen, die Sie beschreiben oder modifizieren. Es macht keinen Sinn, Dateien auf einem Server zu modifizieren und kurze Zeit später dieselben Dateien auf einem anderen Server erneut zu modifizieren. Der Vorteil ist der, dass der beste verfügbare Server automatisch verwendet wird und kein Handeln des Benutzers erforderlich ist.

Wenn die Dateisysteme als Replikationen konfiguriert sind (siehe „Was ist ein repliziertes Dateisystem?“ auf Seite 203), haben die Clients den Vorteil, das Failover verwenden zu können. Beim Failover wird nicht nur automatisch der beste Server bestimmt: Wenn dieser Server ausfällt, verwendet der Client automatisch den nächstbesten Server.

Ein Beispiel für die Konfiguration eines effizienten Dateisystems als Replikation sind Manpages. In einem großen Netzwerk können mehrere Server die aktuellen Manpages exportieren. Von welchem Server aus Sie die Manpages einhängen, spielt keine Rolle, wenn der

Server in Betrieb ist und seine Dateisysteme exportiert. Im vorangegangenen Beispiel werden mehrere Einhängepositionen in einer Liste von Einhängepositionen in einem Map-Eintrag definiert.

```
/usr/man -ro oak:/usr/man rose:/usr/man willow:/usr/man
```

In diesem Beispiel können Sie die Manpages von den Servern `oak`, `rose` oder `willow` einhängen. Welcher Server der beste ist, hängt von verschiedenen Faktoren ab, darunter folgende:

- Die Anzahl von Servern, die eine bestimmte NFS-Protokollebene unterstützen
- Die Nähe des Servers
- Die Gewichtung

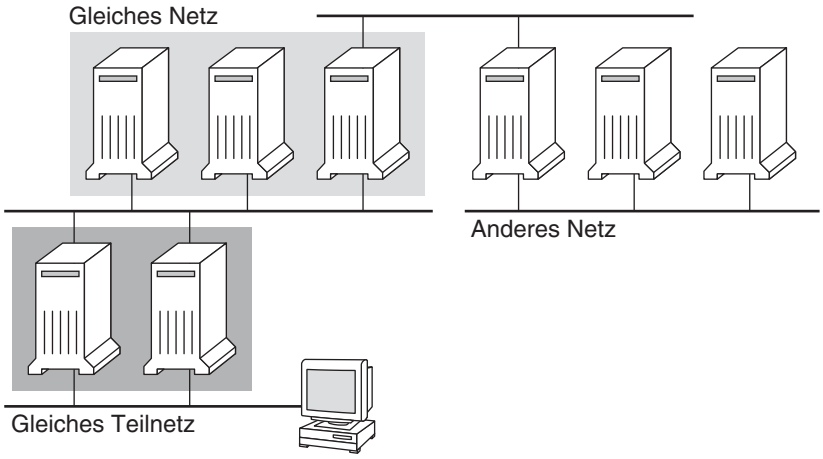
Während des Sortierprozesses werden die Server gezählt, die jede Version des NFS-Protokolls unterstützen. Die Version des Protokolls, die von den meisten Servern unterstützt wird, wird als standardmäßiges Protokoll verwendet. Dadurch wird dem Client die maximale Auswahl an Servern zur Verfügung gestellt.

Nachdem der größte Teil der Server mit derselben Protokollversion gefunden wurde, wird die Liste dieser Server nach Nähe sortiert. Zur Bestimmung der Nähe werden IPv4-Adressen untersucht. Die IPv4-Adressen zeigen an, welche Server sich in jedem Teilnetz befinden. Servern in einem lokalen Teilnetz wird der Vorzug vor Servern in einem Remote-Teilnetz gegeben. Durch die bevorzugte Verwendung des nächsten Servers werden Latenz und Netzwerkverkehr verringert.

Hinweis – Die Nähe kann nicht für Replikationen bestimmt werden, die IPv6-Adressen verwenden.

Abbildung 6–5 zeigt die Servernähe.

ABBILDUNG 6–5 Servernähe



Wenn mehrere Server, die dasselbe Protokoll unterstützen, sich im selben Teilnetz befinden, wird die Dauer zur Herstellung der Verbindung mit jedem Server ermittelt und es wird der schnellste Server verwendet. Das Sortieren kann auch durch die Gewichtung beeinflusst werden (siehe „Autofs und Gewichtung“ auf Seite 226).

Wenn beispielsweise mehr Server der Version 4 zur Verfügung stehen, wird Version 4 als standardmäßiges Protokoll verwendet. Der Sortierprozess ist nun jedoch komplexer. Es folgen einige Beispiele zur Funktionsweise des Sortierprozesses:

- Servern in einem lokalen Teilnetz wird der Vorzug vor Servern in einem Remote-Teilnetz gegeben. Wenn sich also ein Server der Version 3 im lokalen Teilnetz befindet und sich der nächste Server der Version 4 in einem Remote-Teilnetz befindet, wird dem Server der Version 3 der Vorzug gegeben. Wenn zum lokalen Teilnetz Server der Version 2 gehören, erhalten diese den Vorzug vor den Servern der Version 3 und 4 in Remote-Teilnetzen.
- Wenn zum lokalen Teilnetz Server der Version 2, 3 und 4 gehören, ist eine weitere Sortierung erforderlich. Der Automounter zieht die höchste Version im lokalen Teilnetz vor. In diesem Fall ist dies Version 4. Wenn im lokalen Teilnetz jedoch mehr Server der Version 3 oder der Version 2 als Server der Version 4 vorhanden sind, wählt der Automounter die nächstniedrige Version im Verhältnis zur höchsten Version. Wenn beispielsweise im lokalen Teilnetz drei Server der Version 4, drei Server der Version 3 und zehn Server der Version 2 enthalten sind, wird ein Server der Version 3 gewählt.
- Wenn im lokalen Teilnetz mehrere Server der Version 2 und 3 enthalten sind, sucht der Automounter zunächst nach der höchsten Version. Dann zählt der Automounter die Server, die die einzelnen Versionen ausführen. Wenn die höchste Version von den meisten Servern ausgeführt wird, wird die höchste Version gewählt. Wenn eine niedrigere Version von mehr Servern ausgeführt wird, wählt der Automounter ausgehend von der höchsten

Version die nächstniedrige Version. Wenn beispielsweise mehr Server der Version 2 als Server der Version 3 im lokalen Teilnetz vorhanden sind, wird ein Server der Version 2 gewählt.

Hinweis – Die Gewichtung wird auch durch die Werte der Schlüsselwörter in der `/etc/default/nfs`-Datei beeinflusst. Insbesondere können manche Versionen durch die Werte für NFS_SERVER_VERSMIN, NFS_CLIENT_VERSMIN, NFS_SERVER_VERSMAX und NFS_CLIENT_VERSMAX aus dem Sortierprozess ausgeschlossen werden. Weitere Informationen zu diesen Schlüsselwörtern finden Sie unter „Schlüsselwörter für die /etc/default/nfs-Datei“ auf Seite 144.

Bei einem Failover wird der Sortierprozess zum Zeitpunkt des Einhängens überprüft, wenn ein Server ausgewählt wird. In einer Umgebung, in der einzelne Server ihre Dateisysteme nicht temporär exportieren können, eignet sich der Einsatz von mehreren Speicherorten.

Das Failover ist vor allem in einem großen Netzwerk mit vielen Teilnetzen sinnvoll. Autofs wählt einen geeigneten Server aus und kann den NFS-Netzwerkverkehr auf ein Segment des lokalen Netzwerks beschränken. Wenn ein Server mehrere Netzwerkschnittstellen hat, können Sie den Hostnamen auflisten, der jeder Netzwerkschnittstelle zugeordnet ist, als ob die Schnittstelle ein separater Server wäre. Autofs wählt die Schnittstelle, die dem Client am nächsten ist.

Hinweis – Bei manuellen Einhängungen werden weder die Gewichtung noch die Nähe geprüft. Mit dem Befehl `mount` werden die von links nach rechts aufgelisteten Server priorisiert.

Weitere Informationen finden Sie auf der Manpage `automount(1M)`.

Autofs und Gewichtung

Sie können die Auswahl von Servern mit der gleichen Nähe beeinflussen, indem Sie einen Gewichtungswert in die autofs-Map einfügen. Beispiel:

```
/usr/man -ro oak,rose(1),willow(2):/usr/man
```

Die in Klammern eingeschlossenen Werte zeigen die Gewichtung an. Server ohne Gewichtung haben den Wert null und werden darum mit größter Wahrscheinlichkeit ausgewählt. Je höher der Gewichtungswert, desto geringer die Wahrscheinlichkeit, dass der Server ausgewählt wird.

Hinweis – Alle anderen Serverauswahlfaktoren sind wichtiger als die Gewichtung. Die Gewichtung wird nur dann berücksichtigt, wenn aus Servern mit der gleichen Netzwerknähe ausgewählt wird.

Variablen in einem Map-Eintrag

Sie können eine clientspezifische Variable erstellen, indem Sie ein Dollarzeichen (`$`) vor den Namen der Variablen setzen. Mithilfe der Variablen können Sie verschiedene Architekturtypen bereitstellen, die auf den gleichen Dateisystemspeicherort zugreifen. Sie können auch geschweifte Klammern verwenden, um den Namen von angehängten Buchstaben oder Ziffern abzugrenzen. In Tabelle 6–2 werden die vordefinierten Map-Variablen dargestellt.

TABELLE 6–2 Vordefinierte Map-Variablen

Variable	Bedeutung	Abgeleitet von	Beispiel
`ARCH`	Architekturtyp	`uname -m`	`sun4`
`CPU`	Prozessortyp	`uname -p`	`sparc`
`HOST`	Hostname	`uname -n`	`dinky`
`OSNAME`	Betriebssystemname	`uname -s`	`SunOS`
`OSREL`	Betriebssystemversion	`uname -r`	`5.8`
`OSVERS`	Betriebssystemsversion	`uname -v`	`GENERIC`

Sie können Variablen überall auf der Eintragszeile verwenden, jedoch nicht als Schlüssel. Sie verwenden beispielsweise einen Dateiserver, der Binärwerte für SPARC- und x86-Architekturen aus `/usr/local/bin/sparc` und `/usr/local/bin/x86` exportiert. Die Clients können Einhängungen über einen Map-Eintrag wie den folgenden ausführen:

```
/usr/local/bin        -ro     server:/usr/local/bin/$CPU
```

Jetzt gilt der auf die Clients bezogene Eintrag für alle Architekturen.

Hinweis – Die meisten Anwendungen, die für eine der sun4-Architekturen entwickelt wurden, können auf allen sun4-Plattformen ausgeführt werden. Die `-ARCH`-Variable ist für `sun4` festcodiert.

Maps, die sich auf andere Maps beziehen

Ein in einer Datei-Map verwendeter Map-Eintrag +*mapname* bewirkt, dass automount die angegebene Map liest, als wäre sie in der aktuellen Datei enthalten. Wenn vor *mapname* kein Schrägstrich steht, behandelt autofs den Map-Namen als Zeichenfolge und verwendet die Name Service Switch-Richtlinie, um nach dem Map-Namen zu suchen. Wenn der Pfadname ein absoluter Pfadname ist, sucht `automount` in einer lokalen Map, um den Namen zu finden. Wenn die Map mit einem Bindestrich (-) beginnt, fragt `automount` die entsprechende integrierte Map wie beispielsweise `hosts` ab.

Diese Name Service Switch-Datei enthält einen Eintrag für autofs mit der Bezeichnung `automount`, in dem die Reihenfolge angegeben ist, in der nach dem Name Service gesucht wurde. Die folgende Datei ist ein Beispiel für eine Name Service Switch-Datei:

```
#
# /etc/nsswitch.nis:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it uses NIS (YP) in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the /etc/netconfig
# file contains "switch.so" as a nametoaddr library for "inet" transports.
# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:         files nis
group:          files nis

# consult /etc "files" only if nis is down.
hosts:          nis [NOTFOUND=return] files
networks:       nis [NOTFOUND=return] files
protocols:      nis [NOTFOUND=return] files
rpc:            nis [NOTFOUND=return] files
ethers:         nis [NOTFOUND=return] files
netmasks:       nis [NOTFOUND=return] files
bootparams:     nis [NOTFOUND=return] files
publickey:      nis [NOTFOUND=return] files
netgroup:       nis
automount:      files nis
aliases:        files nis
# for efficient getservbyname() avoid nis
services:       files nis
```

In diesem Beispiel werden die lokalen Maps vor den NIS-Maps durchsucht. Darum können in Ihrer lokalen `/etc/auto_home`-Map einige Einträge für die Home-Verzeichnisse enthalten sein, auf die am häufigsten zugegriffen wird. Sie können dann den Switch verwenden, um zur NIS-Map zurückzukehren, um auf die anderen Einträge zuzugreifen.

```
bill              cs.csc.edu:/export/home/bill
bonny             cs.csc.edu:/export/home/bonny
```

Wenn nach der Abfrage der einbezogenen Map keine Übereinstimmung gefunden wird, fährt `automount` mit der Abfrage der aktuellen Map fort. Darum können Sie mehrere Einträge nach einem +-Eintrag einfügen.

```
bill                cs.csc.edu:/export/home/bill
bonny               cs.csc.edu:/export/home/bonny
+auto_home
```

Die einbezogene Map kann eine lokale Datei oder eine integrierte Map sein. Beachten Sie, dass nur in lokalen Dateien +-Einträge enthalten sein können.

```
+auto_home_finance      # NIS+ map
+auto_home_sales        # NIS+ map
+auto_home_engineering  # NIS+ map
+/etc/auto_mystuff      # local map
+auto_home              # NIS+ map
+-hosts                 # built-in hosts map
```

Hinweis – Sie können keine +-Einträge in NIS+- oder NIS-Maps verwenden.

Ausführbare autofs-Maps

Sie können eine autofs-Map erstellen, mit deren Hilfe Befehle zum Generieren der autofs-Einhängepunkte ausgeführt werden. Sie können aus der Verwendung einer ausführbaren autofs-Map Nutzen ziehen, wenn Sie die autofs-Struktur aus einer Datenbank oder einer unstrukturierten Datei erstellen müssen. Der Nachteil der Verwendung einer ausführbaren Map besteht darin, dass die Map auf jedem Host installiert werden muss. Eine ausführbare Map kann weder in den NIS- noch in den NIS+-Name Service einbezogen werden.

Die ausführbare Map muss einen Eintrag in der `auto_master`-Datei haben.

```
/execute    auto_execute
```

Es folgt ein Beispiel einer ausführbaren Map:

```
#!/bin/ksh
#
# executable map for autofs
#

case $1 in
            src)  echo '-nosuid,hard bee:/export1' ;;
esac
```

Damit dieses Beispiel funktioniert, muss die Datei als `/etc/auto_execute` installiert sein, und das ausführbare Bit muss gesetzt sein. Setzen Sie die Berechtigungen auf `744`. In diesem Fall bewirkt die Ausführung des Befehls, dass das `/export1` -Dateisystem von `bee` eingehängt wird:

```
% ls /execute/src
```

Modifizieren, wie autofs im Netzwerk navigiert (Modifizieren von Maps)

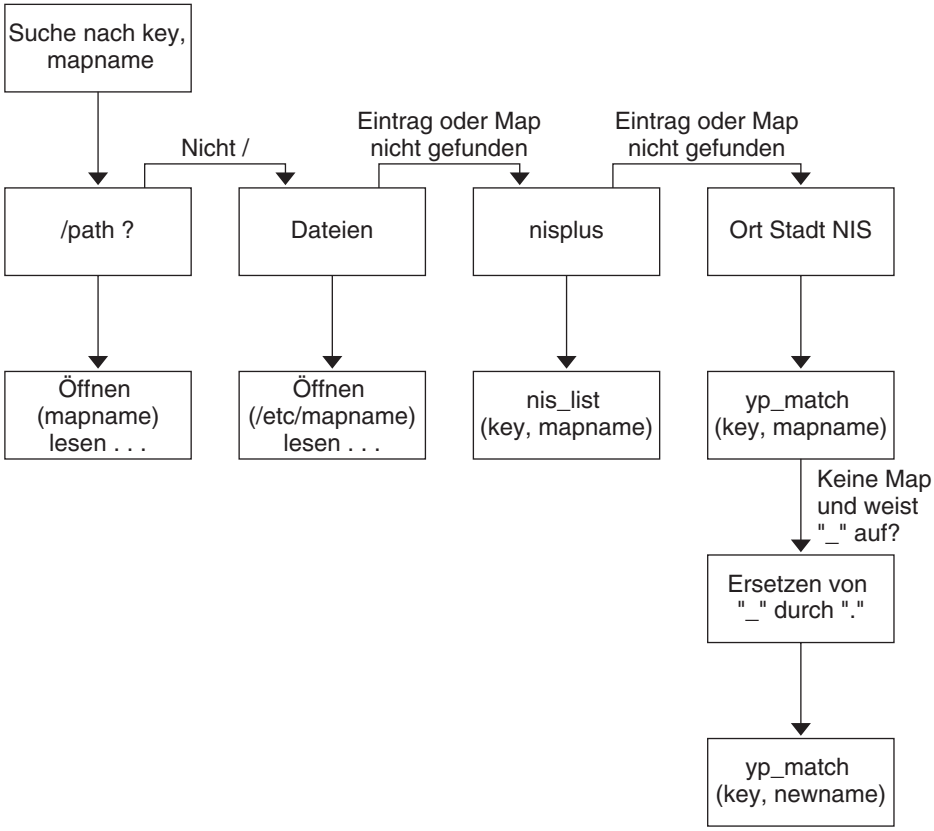
Sie können Einträge in Maps modifizieren, löschen oder hinzufügen, um die Anforderungen in Ihrer Umgebung zu erfüllen. Da sich der Speicherort von Anwendungen und anderen Dateisystemen, die von Benutzern benötigt werden, ändert, müssen diese Änderungen in den Maps reflektiert werden. Sie können autofs-Maps jederzeit modifizieren. Ob Ihre Modifizierungen beim nächsten Einhängen eines Dateisystems durch `automountd` wirksam sind, hängt davon ab, welche Map Sie modifizieren und welcher Art die von Ihnen vorgenommenen Modifizierungen sind.

Standardmäßiges Verhalten von autofs bei Verwendung von Name Services

Während des Boot-Vorgangs wird autofs vom Service `svc:/system/filesystem/autofs` aufgerufen. Dann prüft autofs die Master-Map `auto_master`. Autofs unterliegt den nachstehend erläuterten Regeln.

Autofs verwendet den Name Service, der im automount-Eintrag der `/etc/nsswitch.conf`-Datei angegeben ist. Wenn NIS+ angegeben ist, aber nicht die lokalen Dateien oder NIS, werden alle Map-Namen in der vorliegenden Form verwendet. Wenn NIS angegeben ist und autofs keine passende Map, aber einen Map-Namen findet, der einen oder mehrere Unterstriche enthält, werden die Unterstriche in Punkte umgewandelt. Durch diese Änderung können die alten NIS-Dateinamen verwendet werden. Anschließend prüft autofs erneut die Map (siehe Abbildung 6–6).

ABBILDUNG 6–6 Wie autofs den Name Service verwendet



Die Bildschirmaktivität in dieser Sitzung sieht wie im folgenden Beispiel aus:

```
$ grep /home /etc/auto_master
/home           auto_home

$ ypmatch brent auto_home
Can't match key brent in map auto_home.  Reason: no such map in
server's domain.

$ ypmatch brent auto.home
diskus:/export/home/diskus1/&
```

Wenn Dateien als Name Service ausgewählt werden, wird vorausgesetzt, dass es sich bei allen Maps um lokale Dateien im `/etc`-Verzeichnis handelt. Autofs interpretiert einen mit einem Schrägstrich (`/`) beginnenden Map-Namen als lokal, ungeachtet des von autofs verwendeten Name Service.

Autofs-Referenz

In den übrigen Abschnitten dieses Kapitels werden weiter fortgeschrittene Funktionen und Themen im Zusammenhang mit autofs behandelt.

Autofs und Metazeichen

Autofs erkennt die besondere Bedeutung mancher Zeichen. Manche Zeichen werden für Ersetzungen verwendet, andere werden verwendet, um andere Zeichen vor dem autofs-Map-Parser zu schützen.

Und-Zeichen (&)

Wenn Sie eine Map wie die folgende verwenden, in der viele Unterverzeichnisse angegeben sind, sollten Sie die Ersetzung von Zeichenfolgen in Erwägung ziehen.

```
john        willow:/home/john
mary        willow:/home/mary
joe         willow:/home/joe
able        pine:/export/able
baker       peach:/export/baker
```

Sie können das Und-Zeichen (&) verwenden, um den Schlüssel zu ersetzen, ganz gleich, wo dieser zu finden ist. Wenn Sie das Und-Zeichen verwenden, wird die Map geändert und hat dann folgendes Aussehen:

```
john        willow:/home/&
mary        willow:/home/&
joe         willow:/home/&
able        pine:/export/&
baker       peach:/export/&
```

Auch können Sie Schlüsselersetzungen in einer direkten Map verwenden, wenn ein Fall wie der folgende gegeben ist:

```
/usr/man                        willow,cedar,poplar:/usr/man
```

Zudem können Sie den Eintrag wie folgt weiter vereinfachen:

```
/usr/man                        willow,cedar,poplar:&
```

Beachten Sie, dass bei einer Ersetzung des Und-Zeichens die gesamte Schlüsselzeichenfolge verwendet wird. Wenn der Schlüssel in einer direkten Map mit einem Schrägstrich (/) beginnt (was normalerweise der Fall sein sollte), wird dieser in die Ersetzung einbezogen. Dementsprechend ist die folgende Angabe nicht möglich:

```
/progs              &1,&2,&3:/export/src/progs
```

Der Grund dafür ist, dass autofs das Beispiel wie folgt interpretieren würde:

```
/progs                  /progs1,/progs2,/progs3:/export/src/progs
```

Sternchen (*)

Sie können das Sternchen (* als universelles Ersetzungszeichen verwenden, um jeden Schlüssel anzupassen. Mithilfe dieses Map-Eintrags können Sie das `/export`-Dateisystem von allen Hosts einhängen.

```
*                         &:/export
```

Jedes Und-Zeichen wird durch den Wert eines Schlüssels ersetzt. Autofs interpretiert das Sternchen als Dateiende-Zeichen.

Autofs und Sonderzeichen

Wenn Sie einen Map-Eintrag verwenden, der Sonderzeichen enthält, müssen Sie eventuell Verzeichnisse einhängen, die Namen haben, die den autofs-Map-Parser verwirren. Der autofs-Parser kann beispielsweise Namen, die Doppelpunkte, Kommas und Leerzeichen enthalten, nicht richtig verarbeiten. Diese Namen sollten wie folgt in doppelte Anführungszeichen gesetzt werden:

```
/vms    -ro    vmsserver: -  -  - "rc0:dk1 - "
/mac    -ro    gator:/ - "Mr Disk - "
```

TEIL III

SLP (Service Location Protocol) – Themen

Dieser Abschnitt enthält eine Übersicht, Planungsinformationen, aufgabenbezogene Informationen sowie Referenzinformationen zum (SLP)-Service (Service Location Protocol).

◆ ◆ ◆ KAPITEL 7

7 SLP (Übersicht)

Das Service Location Protocol (SLP) stellt eine übertragbare, plattformunabhängige Struktur für die Erkennung und Bereitstellung von SLP-fähigen Netzwerkdiensten bereit. In diesem Kapitel werden die SLP-Architektur und die Solaris-Implementierung von SLP für IP-Intranets beschrieben.

- „SLP-Architektur“ auf Seite 237
- „SLP-Implementierung“ auf Seite 240

SLP-Architektur

In diesem Kapitel werden die grundlegende Funktionsweise von SLP sowie die Agenten und Prozesse beschrieben, die in der SLP-Verwaltung verwendet werden.

SLP stellt die folgenden Services automatisch bereit. Die Services müssen nur wenig oder nicht konfiguriert werden.

- Clientanwendungsanforderungen von Informationen, die für den Zugriff auf einen Service erforderlich sind
- Service-Advertisement auf Netzwerkhardware oder Softwareservern, beispielsweise Drucker, Dateiserver, Videokameras und HTTP-Server
- Kontrollierte Wiederherstellung bei Ausfällen von primären Servern

Außerdem haben Sie folgende Möglichkeiten, um die SLP-Funktion zu verwalten und nach Bedarf abzustimmen:

- Organisieren von Services und Benutzern in *Bereichen*, die aus logischen oder funktionellen Gruppen bestehen
- Aktivieren der SLP-Protokollierung, um die SLP-Funktion in Ihrem Netzwerk zu überwachen und Fehler zu beseitigen
- Abstimmen von SLP-Parametern zur zeitlichen Steuerung, um die Leistung und Skalierbarkeit zu erhöhen

- Konfigurieren von SLP, damit keine Multicast-Meldungen gesendet und verarbeitet werden, wenn SLP in Netzwerken bereitgestellt wird, die keine Unterstützung für das Multicast-Routing haben
- Bereitstellen von SLP-Verzeichnisagenten, um die Skalierbarkeit und Leistung zu verbessern

Zusammenfassung des SLP-Konzepts

SLP-Bibliotheken informieren netzwerkorientierte Agenten, die Services bekannt geben, damit diese Services über ein Netzwerk erkannt werden können. SLP-Agenten verfügen über aktuelle Informationen zum Typ und zum Standort von Services. Diese Agenten können auch Proxyregistrierungen verwenden, um Services bekannt zu geben, die nicht direkt für SLP aktiviert sind. Weitere Informationen finden Sie in Kapitel 10, „Integrieren von veralteten Services“.

Clientanwendungen verwenden SLP-Bibliotheken, die Anforderungen direkt an die Agenten weitergeben, die Services bekannt geben.

SLP-Agenten und Prozesse

In der folgenden Tabelle werden die SLP-Agenten beschrieben. Definitionen der hier verwendeten Begriffe und anderer Begriffe, die im vorliegenden Dokument verwendet werden, finden Sie im Glossar.

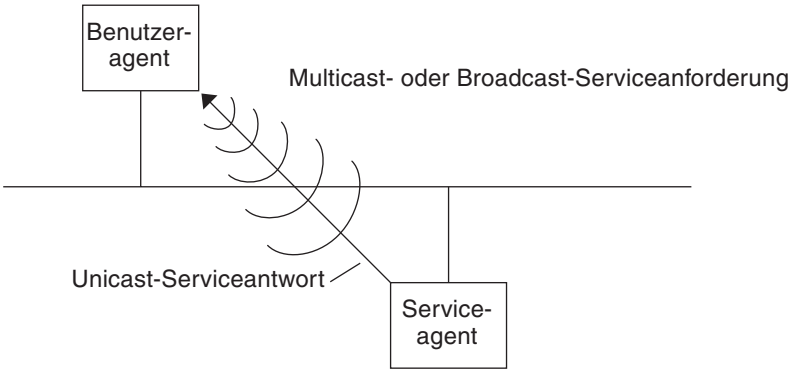
TABELLE 7–1 SLP-Agenten

SLP-Agent	Beschreibung
Verzeichnisagent (Directory Agent, DA)	Ein Prozess zum Zwischenspeichern von SLP-Advertisements, die von Serviceagenten (SAs) registriert werden. Der DA leitet auf Anforderung Service-Advertisements an Benutzeragenten (UAs) weiter.
Serviceagent (Service Agent, SA)	Ein SLP-Agent, der anstelle eines Service handelt, um Service-Advertisements auszugeben und den Services mit Verzeichnisagenten (DAs) zu registrieren
Benutzeragent (User Agent, UA)	Ein SLP-Agent, der anstelle eines Benutzers oder einer Anwendung handelt, um Informationen zum Service-Advertisement zu erhalten
Bereich	Eine administrative oder logische Gruppierung von Services

Die folgende Abbildung zeigt die wichtigsten Agenten und Prozesse, die zur Implementierung der SLP-Architektur dienen. Es handelt sich um eine standardmäßige Bereitstellung von SLP. Eine spezielle Konfiguration wurde nicht durchgeführt. Es sind nur zwei Agenten erforderlich: der UA und der SA. Die SLP-Struktur ermöglicht dem UA, mehrere Serviceanforderungen an

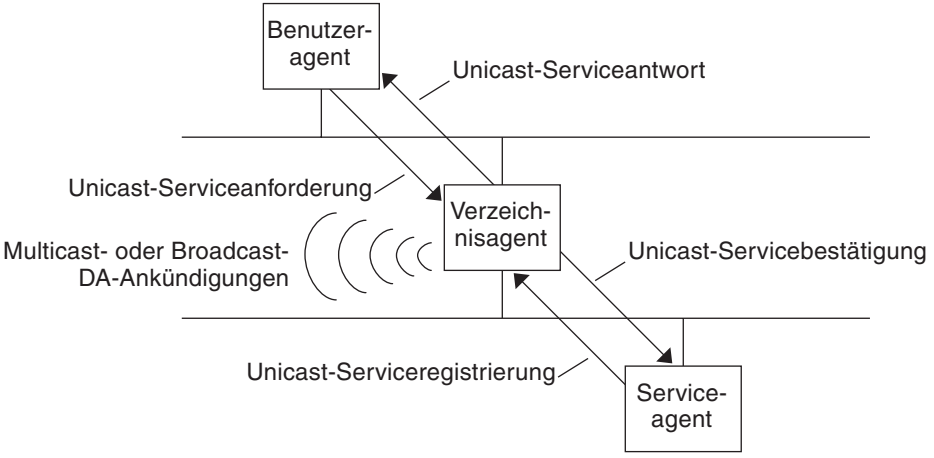
den SA zu senden. Der SA sendet eine Antwort an den UA. Wenn der UA beispielsweise eine Serviceanforderung sendet, antwortet der SA mit einer servicebezogenen Antwort. In der servicebezogenen Antwort ist der Standort der Services enthalten, die den Anforderungen des Clients entsprechen. Andere Anforderungen und Antworten sind möglich, wenn es um Attribute und Servicetypen geht. Weitere Informationen finden Sie in Kapitel 11, „SLP (Referenz)“.

ABBILDUNG 7–1 Wichtige SLP-Agenten und Prozesse



Die folgende Abbildung zeigt die wichtigsten Agenten und Prozesse, die zur Implementierung der SLP-Architektur dienen, wenn ein DA in der Struktur bereitgestellt wird.

ABBILDUNG 7–2 Implementierung von Agenten und Prozessen in der SLP-Architektur mit einem DA



Wenn Sie DAs bereitstellen, werden weniger Meldungen über das Netzwerk gesendet und UAs können Informationen viel schneller abrufen. DAs sind wichtig, wenn die Größe eines Netzwerks zunimmt oder keine Unterstützung für das Multicast-Routing vorhanden ist. Der DA dient als Cache für registrierte Service-Advertisements. SAs senden Registrierungsmeldungen (`SrvReg`), in denen alle Services aufgelistet sind, die den DAs bekannt gegeben werden. Als Antwort auf diese Meldungen erhalten die SAs Bestätigungen (`SrvAck`). Die Service-Advertisements werden mit dem DA aktualisiert, oder sie verfallen entsprechend der jeweils festgelegten Lebensdauer. Nachdem ein UA einen DA erkannt hat, sendet der UA eine Anforderung an den DA (anstelle von mehrfachen Anforderungen an SAs).

Weitere Informationen zu Solaris-SLP-Meldungen finden Sie in Kapitel 11, „SLP (Referenz)“.

SLP-Implementierung

In der SLP-Implementierung von Solaris werden die SLP-SAs, UAs, DAs, SA-Server, Bereiche und andere architektonischen Komponenten, die in Tabelle 7–1 aufgeführt sind, teilweise `slpd` und teilweise Anwendungsprozessen zugeordnet. Der SLP-Dämon, `slpd`, organisiert bestimmte SLP-Interaktionen außerhalb des Hosts, um folgende Vorgänge auszuführen:

- Passive und aktive Verzeichnisagenterkennung, um alle DAs im Netzwerk zu erkennen
- Führen einer aktualisierten Tabelle von DAs zur Verwendung der UAs und SAs auf dem lokalen Host
- Fungieren als SA-Proxyserver für veraltete Service-Advertisements (Proxyregistrierung)

Sie können die `net.slpisDA`-Eigenschaft definieren, damit auch `slpd` als DA fungiert. Lesen Sie dazu Kapitel 9, „Verwalten von SLP (Aufgaben)“.

Weitere Informationen zum SLP-Dämon finden Sie auf der Manpage `slpd(1M)`.

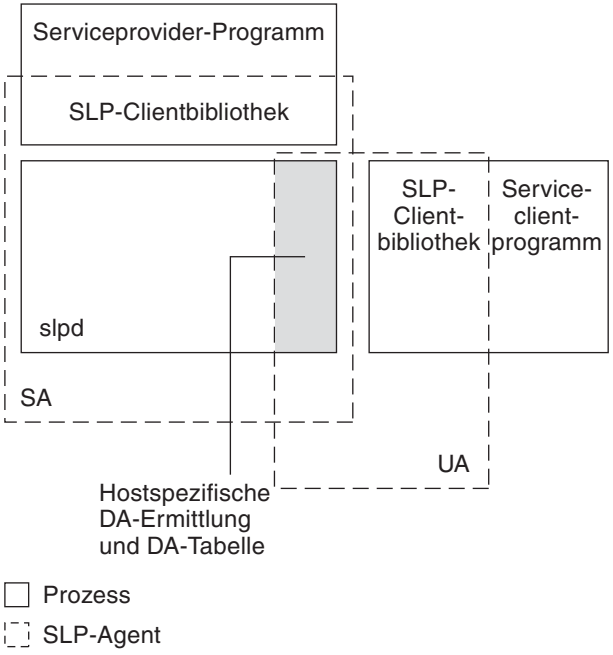
Neben `slpd` ermöglichen die C/C++- und Java-Clientbibliotheken (`libslp.so` und `slp.jar`) den Zugriff auf die SLP-Struktur für UA- und SA-Clients. Die Client-bibliotheken bieten folgende Funktionen:

- Software mit Netzwerkdiensten, die Service-Advertisements registrieren und die Registrierung dieser entfernen können
- Clientsoftware, die Services anfordern kann, indem Service-Advertisements abgefragt werden
- Die Liste der SLP-Bereiche, die für die Registrierung und Anforderungen zur Verfügung stehen

Es ist keine spezielle Konfiguration erforderlich, um die prozessinterne Kommunikation von `slpd` und den Clientbibliotheken herzustellen. Sie müssen jedoch zunächst den `slpd`-Prozess ausführen, bevor Sie die Clientbibliotheken laden, damit die Bibliotheken funktionieren.

In der folgenden Abbildung verwendet die SLP-Clientbibliothek im Serviceprovider-Programm die SA-Funktion. Das Serviceprovider-Programm verwendet die SLP-Clientbibliothek, um Services mit `slpd` zu registrieren und die Registrierung dieser zu entfernen. Die SLP-Clientbibliothek im Serviceclient-Programm verwendet die UA-Funktion. Das Serviceclient-Programm verwendet die SLP-Clientbibliothek, um Anforderungen auszugeben. Die SLP-Clientbibliothek versendet entweder Anforderungen an mehrere SAs oder Anforderungen an einzelne DAs. Diese Art der Kommunikation ist für die Anwendung transparent, allerdings geht die Einzelversendung von Anforderungen schneller vonstatten. Das Verhalten der Clientbibliothek kann durch verschiedenen SLP-Konfigurationseigenschaften beeinflusst werden. Weitere Informationen finden Sie in Kapitel 9, „Verwalten von SLP (Aufgaben)“. Der `slpd`-Prozess steuert alle SA-Funktionen, wie beispielsweise die Beantwortung von Multicast-Anforderungen und die Registrierung mit DAs.

ABBILDUNG 7–3 SLP-Implementierung



Weitere SLP-Informationsquellen

In den folgenden Dokumenten finden Sie weitere Informationen zu SLP:

- Kempf, James und Pete St. Pierre. *Service Location Protocol for Enterprise Networks*. John Wiley & Sons, Inc. ISBN-Nummer: 0–471–31587–7.
- *Authentication Management Infrastructure Administration Guide*. Teilenummer: 805–1139–03.
- Guttman, Erik, Charles Perkins, John Veizades und Michael Day. *Service Location Protocol, Version 2, RFC 2608* von der Internet Engineering Task Force (IETF). [http://www.ietf.org/rfc/rfc2608.txt]
- Kempf, James und Erik Guttman. *An API for Service Location, RFC 2614* von der Internet Engineering Task Force (IETF). [http://www.ietf.org/rfc/rfc2614.txt]

◆ ◆ ◆ KAPITEL 8

Planen und Aktivieren von SLP (Aufgaben)

Dieses Kapitel enthält Informationen zur Planung und Aktivierung von SLP. In den folgenden Abschnitten werden die SLP-Konfiguration und der Prozess der Aktivierung von SLP erläutert.

- „Überlegungen zur SLP-Konfiguration“ auf Seite 243
- „Verwenden von snoop zur Überwachung von SLP-Aktivitäten“ auf Seite 244

Überlegungen zur SLP-Konfiguration

Der SLP-Dämon ist standardmäßig vorkonfiguriert. Wenn sich die Standardeinstellungen in Ihrem Unternehmen gut bewährt haben, erfordert die Bereitstellung von SLP so gut wie keine weiteren Konfigurationen.

In manchen Fällen jedoch ist es notwendig, die SLP-Eigenschaften zu modifizieren, um Netzwerkvorgänge abzustimmen oder bestimmte Funktionen zu aktivieren. Mit nur wenigen Konfigurationänderungen können Sie beispielsweise die SLP-Protokollierung aktivieren. Die Informationen in einem SLP-Protokoll und in `snoop`-Ablaufverfolgungen geben Ihnen Aufschluss darüber, ob weitere Konfigurationen notwendig sind.

Die SLP-Konfigurationseigenschaften sind in der `slp.conf`-Datei enthalten, die sich im `/etc/inet`-Verzeichnis befindet. Wenn Sie die standardmäßigen Eigenschaftseinstellungen ändern müssen, wenden Sie die entsprechenden Verfahren an, die in Kapitel 9, „Verwalten von SLP (Aufgaben)“ beschrieben werden.

Bevor Sie die SLP-Konfigurationseinstellungen ändern, sollten Sie die folgenden Fragen im Hinblick auf wichtige Aspekte der Netzwerkverwaltung beantworten:

- Welche Netzwerktechnologien werden im Unternehmen eingesetzt?
- Wie viel Netzwerkdatenverkehr können die Technologien problemlos bewältigen?
- Wie viele Services und welche Art von Services stehen im Netzwerk zur Verfügung?

- Wie viele Benutzer hat das Netzwerk? Welche Services werden von den Benutzern benötigt? Wo befinden sich die Benutzer in Relation zu den Services, auf die am häufigsten zugegriffen wird?

Wann eine Neukonfiguration nötig ist

Sie können das SLP-fähige snoop-Dienstprogramm sowie die SLP-Protokollierungsdienstprogramme verwenden, um zu entscheiden, ob eine Neukonfiguration nötig ist und welche Eigenschaften modifiziert werden müssen. Sie können beispielsweise bestimmte Eigenschaften neu konfigurieren, um folgende Aufgaben zu erfüllen:

- Verwenden diverser Netzwerkmedien, die verschiedene Latenzen und Bandbreiteneigenschaften aufweisen
- Wiederherstellung bei Netzwerkausfällen oder ungeplanter Partitionierung
- Hinzufügen von DAs, um die Ausbreitung von SLP-Multicast-Vorgängen zu verringern
- Implementieren neuer Bereiche, um Benutzer und die Bereiche zu organisieren, auf die am häufigsten zugegriffen wird

Verwenden von snoop zur Überwachung von SLP-Aktivitäten

Das snoop-Dienstprogramm ist ein passives Verwaltungstool, das Netzwerkverkehrsinformationen bereitstellt. Das Dienstprogramm selbst ruft minimalen Datenverkehr hervor und ermöglicht Ihnen, alle in Ihrem Netzwerk stattfindenden Aktivitäten zu überwachen.

Mit dem snoop-Dienstprogramm kann der aktuelle SLP-Meldungsdatenverkehr verfolgt werden. Wenn Sie beispielsweise snoop in Verbindung mit dem Befehlszeilenargument `slp` ausführen, zeigt das Dienstprogramm Ablaufverfolgungen mit Informationen zu SLP-Registrierungen und zur Entfernung dieser an. Sie können diese Informationen verwenden, um die Netzwerkbelastung zu bestimmen, indem Sie überprüfen, welche Services registriert sind und wie viele Registrierungsaktivitäten stattfinden.

Das snoop-Dienstprogramm dient auch der Überwachung des Datenverkehrsflusses zwischen SLP-Hosts in Ihrem Unternehmen. Wenn Sie snoop in Verbindung mit dem Befehlszeilenargument slp ausführen, können Sie die folgenden SLP-Aktivitäten überwachen, um festzustellen, ob eine Neukonfiguration des Netzwerks oder des Agenten nötig ist:

- Die Anzahl von Hosts, die einen bestimmten DA verwenden. Anhand dieser Informationen können Sie entscheiden, ob zusätzliche DAs für den Lastausgleich bereitgestellt werden müssen.
- Die Anzahl von Hosts, die einen bestimmten DA verwenden. Anhand dieser Informationen können Sie entscheiden, ob bestimmte Hosts mit neuen oder anderen Bereichen konfiguriert werden müssen.
- Überwachung der Zeitüberschreitungen, die ein UA auslöst, oder langsamer DA-Bestätigungen. Sie können feststellen, ob ein DA überlastet ist, indem Sie UA-Zeitüberschreitungen und Neuübertragungen überwachen. Sie können zudem prüfen, ob der DA länger als nur wenige Sekunden benötigt, um Registrierungsbestätigungen an einen SA zu senden. Verwenden Sie diese Informationen, um die Netzwerkbelastung bei Bedarf auszugleichen, durch die der DA beeinträchtigt wird, indem Sie weitere DAs bereitstellen oder die Bereichskonfigurationen ändern.

Wenn Sie snoop in Verbindung mit dem Befehlszeilenargument -V (ausführlich) verwenden, können Sie die Lebensdauer von Registrierungen und den Wert des Aktualisierungs-Flag in SrvReg abrufen, um festzustellen, ob die Anzahl von Neuregistrierungen verringert werden muss.

snoop können Sie auch dazu verwenden, um eine andere Art des SLP-Datenverkehrs zu verfolgen, z. B.:

- Datenverkehr zwischen UA-Clients und DAs
- Datenverkehr zwischen Multicast-UA-Clients und antwortenden DAs

Weitere Informationen zu snoop finden Sie auf der Manpage snoop(1M).

Tipp – Verwenden Sie den Befehl netstat in Verbindung mit snoop, um Datenverkehrs- und Überlastungsstatistiken anzuzeigen. Weitere Informationen zu netstat finden Sie auf der Manpage netstat(1M).

▼ So verwenden Sie snoop, um SLP-Ablaufverfolgungen auszuführen

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Führen Sie snoop in Verbindung mit dem Befehlszeilenargument slp aus.

```
Brief Mode:
# snoop slp
```

Wenn Sie snoop im standardmäßigen *kurzen* Modus ausführen, erscheinen ständig Ausgaben auf Ihrem Bildschirm. SLP-Meldungen werden gekürzt, damit sie pro Ablaufverfolgung auf eine Zeile passen.

```
Verbose Mode:
# snoop -v slp
```

Wenn Sie snoop im *ausführlichen* Modus ausführen, erscheinen ständig von snoop übermittelte ungekürzte Ausgaben auf Ihrem Bildschirm. Dabei werden folgende Informationen angezeigt:

- Die vollständige Adresse der Service-URL
- Alle Serviceattribute
- Die Lebensdauer der Registrierung
- Alle Sicherheitsparameter und Flags (sofern vorhanden)

Hinweis – Sie können das Befehlszeilenargument slp in Verbindung mit anderen snoop-Optionen verwenden.

Analysieren einer snoop slp-Ablaufverfolgung

Im folgenden Beispiel wird slpd im Standardmodus als SA-Server auf *slphost1* ausgeführt. Der SLP-Dämon initialisiert und registriert *slphost2* als Echoserver. Anschließend wird der snoop slp-Prozess auf *slphost1* aufgerufen.

Hinweis – Um die Beschreibung der Ablaufverfolgungsergebnisse zu vereinfachen, sind die Zeilen in der folgenden snoop-Ausgabe mit Zeilennummern versehen.

```
(1) slphost1 -> 239.255.255.253 SLP V@ SrvRqst [24487] service:directory-agent []
(2) slphost2 -> slphost1 SLP V2 DAAdvert [24487] service:directory-agent://129
(3) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(4) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(5) slphost1 -> slphost2 SLP V2 SrvReg [24488/tcp]service:echo.sun:tcp://slphost1:
(6) slphost2 -> slphost1 SLP V2 SrvAck [24488/tcp] ok
(7) slphost1 -> slphost2 SLP V2 SrvDereg [24489/tcp] service:echo.sun:tcp://slphost1:
(8) slphost2 -> slphost1 SLP V2 SrvAck [24489/tcp] ok
```

1. Zeigt slpd auf *slphost1* bei der Durchführung einer aktiven Verzeichnisagenterkennung durch mehrfaches Senden an die SLP-Multicast-Gruppenadresse, während nach Verzeichnisagenten gesucht wird. Die Meldungsnummer 24487 für die aktive Erkennung steht in der Ablaufverfolgung in eckigen Klammern.

2. Zeigt an, dass die Anforderung 24487 einer aktiven Erkennung von Ablaufverfolgung 1 durch den `slpd` beantwortet wird, der als DA auf dem Host *slphost2* ausgeführt wird. Die Service-URL von *slphost2* wurde gekürzt, damit sie auf eine einzelne Zeile passt. Der DA hat ein DA-Advertisement als Antwort auf die Multicast-DA-Erkennungsmeldung gesendet. Dies ist aus den übereinstimmenden Meldungsnummern in den Ablaufverfolgungen 1 und 2 ersichtlich.
3. Zeigt Multicast-Sendungen von den UAs auf *slphost1* für weitere DAs. Da die Anforderung bereits von *slphost2* beantwortet wurde, antwortet er nicht mehr. Andere DAs antworten auch nicht.
4. Wiederholt den in der vorangegangenen Zeile angegebenen Multicast-Vorgang.
5. Zeigt einen `slpd` auf *slphost1*, der SA-Clientregistrierungen an den DA auf *slphost2* sendet. Eine Unicast-Serviceregistrierung (`SrvReg`) für einen Echoserver wird von *slphost1* für den DA auf *slphost2* durchgeführt.
6. Zeigt, dass *slphost2* auf die *slphost1*-`SrvReg`-Meldung mit einer Servicebestätigung (`SrvAck`) antwortet, wodurch angezeigt wird, dass die Registrierung erfolgreich durchgeführt wurde.

   Der Datenverkehr zwischen dem Echoserver, auf dem der SA-Client ausgeführt wird, und dem SLP-Dämon auf *slphost1* wird nicht in der `snoop`-Ablaufverfolgung angezeigt. Dieses Fehlen von Informationen ist darauf zurückzuführen, dass der `snoop`-Vorgang über den Netzwerk-Loopback ausgeführt wird.
7. Zeigt, dass der Echoserver auf *slphost1* die Registrierung des Echoservice-Advertisements entfernt. Der SLP-Dämon auf *slphost1* leitet die Entfernung der Registrierung an den DA auf *slphost2* weiter.
8. Zeigt, dass *slphost2* dem *slphost1* mit einer Servicebestätigung (`SrvAck`) antwortet, die anzeigt, dass die Entfernung der Registrierung erfolgreich durchgeführt wurde.

   Der `/tcp`-Parameter, der an die Meldungsnummer in den Zeilen 5, 6, 7 und 8 angefügt ist, zeigt an, dass der Meldungsaustausch über TCP stattgefunden hat.

Die nächsten Schritte

Nach der Überwachung des SLP-Datenverkehrs können Sie die mithilfe der `snoop`-Ablaufverfolgung gesammelten Informationen verwenden, um festzustellen, ob eine Neukonfiguration der SLP-Standardeinstellungen nötig ist. Zum Konfigurieren der SLP-Eigenschaftseinstellungen verwenden Sie die relevanten Informationen in Kapitel 9, „Verwalten von SLP (Aufgaben)“. Weitere Informationen zur SLP-Meldungsübermittlung und zu Serviceregistrierungen finden Sie in Kapitel 11, „SLP (Referenz)“.

◆ ◆ ◆ KAPITEL 9

Verwalten von SLP (Aufgaben)

Die folgenden Abschnitte enthalten Informationen und Aufgaben zum Konfigurieren von SLP-Agenten und -Prozessen.

- „Konfigurieren von SLP-Eigenschaften“ auf Seite 249
- „Modifizieren der Häufigkeit von DA-Advertisements und -Erkennungen“ auf Seite 252
- „Verwenden verschiedener Netzwerkmedien, Topologien oder Konfigurationen“ auf Seite 257
- „Modifizieren von Zeitüberschreitungseinstellungen bei SLP-Suchanforderungen“ auf Seite 262
- „Bereitstellen von Bereichen“ auf Seite 267
- „Bereitstellen von DAs“ auf Seite 270
- „SLP und Multihoming“ auf Seite 274

Konfigurieren von SLP-Eigenschaften

SLP-Konfigurationseigenschaften dienen zur Steuerung der Netzwerkinteraktionen, der Eigenschaften von SLP-Agenten, von Zuständen und der Protokollierung. In den meisten Fällen muss die standardmäßige Konfiguration dieser Eigenschaften nicht geändert werden. Sie können jedoch die in diesem Kapitel beschriebenen Verfahren anwenden, um Veränderungen des Netzwerks oder der Topologie zu berücksichtigen und folgende Ziele zu erreichen:

- Kompensierung von Netzwerklatenzen
- Verringerung der Netzwerkbelastung
- Hinzufügen von Agenten oder Neuzuweisung von IP-Adressen
- Aktivieren der SLP-Protokollierung

Sie können die SLP-Konfigurationsdatei (`/etc/inet/slp.conf`) bearbeiten, um Vorgänge wie die in der folgenden Tabelle auszuführen.

TABELLE 9–1 SLP-Konfigurationsvorgänge

Vorgang	Beschreibung
Festlegen, ob `slpd` als DA-Server (Directory Agent) fungieren soll: Der SA-Server (Service Agent) ist als Standardserver definiert.	Setzen Sie die `net.slpisDA`-Eigenschaft auf `True`.
Festlegen der zeitlichen Steuerung der DA-Multicast-Meldungen	Legen Sie anhand der `net.slp.DAHeartBeat`-Eigenschaft fest, wie oft ein DA ein nicht angefordertes DA-Advertisement mehrfach versendet.
Aktivieren der DA-Protokollierung zur Überwachung des Netzwerkverkehrs	Setzen Sie die `net.slp.traceDATraffic`-Eigenschaft auf `True` .

Grundelemente der SLP-Konfigurationsdatei

Durch die `/etc/inet/slp.conf`-Datei werden jedesmal alle SLP-Aktivitäten definiert und aktiviert, wenn Sie den SLP-Dämon neu starten. Die Konfigurationsdatei besteht aus folgenden Elementen:

- Konfigurationseigenschaften
- Kommentarzeilen und Notationen

Konfigurationseigenschaften

Alle grundlegenden SLP-Eigenschaften wie beispielsweise `net.slp.isDA` und `net.slp.DAHeartBeat` werden im folgenden Format angegeben:

```
net.slp.<keyword>
```

Das SLP-Verhalten wird durch den Wert einer Eigenschaft oder einer Kombination von Eigenschaften in der `slp.conf`-Datei definiert. Eigenschaften sind als Schlüsselwert-Paare in der SLP-Konfigurationsdatei strukturiert. Wie im folgenden Beispiel dargestellt ist, besteht ein Schlüsselwert-Paar aus einem Eigenschaftsnamen und einem zugehörigen Wert.

```
<property name>=<value>
```

Der Schlüssel für jede Eigenschaft ist der Eigenschaftsname. Der Wert dient zur Angabe numerischer Größen (Distanz oder Zeit), zur Angabe des Status (wahr oder falsch) oder zur Angabe von Zeichenfolgeparametern für die Eigenschaft. Eigenschaftswerte bestehen aus einem der folgenden Dateitypen:

- Wahr/Falsch (Boolesch)
- Ganzzahlen
- Liste von Ganzzahlen
- Zeichenfolgen
- Liste von Zeichenfolgen

Wenn der definierte Wert nicht zulässig ist, wird der Standardwert für den betreffenden Eigenschaftsnamen verwendet. Außerdem wird eine Fehlermeldung mithilfe von syslog protokolliert.

Kommentarzeilen und Notationen

Sie können Kommentare in die `slp.conf`-Datei einfügen, die zur Beschreibung der Eigenschaften und Funktion der betreffenden Zeile dienen. Kommentarzeilen sind optional, können aber hilfreich für die Systemverwaltung sein.

Hinweis – Bei Einstellungen in der Konfigurationsdatei wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie in: Guttman, Erik, James Kempf, and Charles Perkins, Service Templates and service: scheme, RFC 2609 from the Internet Engineering Task Force (IETF). [http://www.ietf.org/rfc/rfc2609.txt]

▼ So ändern Sie Ihre SLP-Konfiguration

Anhand des folgenden Verfahrens können Sie die Eigenschaftseinstellungen in Ihrer SLP-Konfigurationsdatei ändern. Auch mit SLP-fähiger Client- oder Servicesoftware kann die SLP-Konfiguration geändert werden, indem die SLP-API verwendet wird. Diese API ist in "An API for Service Location",RFC 2614, der Internet Engineering Task Force (IETF) dokumentiert. [http://www.ietf.org/rfc/rfc2614.txt]

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Bearbeiten Sie nach Bedarf die Eigenschaftseinstellungen in der `/etc/inet/slp.conf`-Datei.**

   Allgemeine Informationen zu den SLP-Eigenschaftseinstellungen finden Sie unter „Konfigurationseigenschaften“ auf Seite 250. In den Abschnitten, die nach dem hier beschriebenen Verfahren folgen, finden Sie Beispiele für verschiedene Szenarios, in denen Sie die `slp.conf` -Eigenschaften ändern können. Siehe dazu `slp.conf(4)`.

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6 **Starten Sie `slpd` neu, damit Ihre Änderungen wirksam werden.**

```
# svcadm enable network/slp
```

Hinweis – Der SLP-Dämon ruft Informationen aus der Konfigurationsdatei ab, wenn Sie `slpd` stoppen oder starten.

Beispiel 9–1 Einrichten von `slpd`, damit slpd als DA-Server fungieren kann

Sie können die Standardeinstellung des SA-Servers ändern, damit `slpd` als DA-Server fungieren kann, indem Sie die `net.slp.isDA`-Eigenschaft in der `slpd.conf`-Datei auf `True` setzen.

```
net.slp.isDA=True
```

In jedem Bereich steuern zahlreiche Eigenschaften die verschiedenen Aspekte der Konfiguration. In den folgenden Abschnitten werden die verschiedenen Szenarios beschrieben, in denen Sie die standardmäßigen Eigenschaftseinstellungen ändern können, die in der SLP-Konfiguration verwendet werden.

Modifizieren der Häufigkeit von DA-Advertisements und -Erkennungen

In Situationen wie der folgenden können Sie Eigenschaften modifizieren, die zur zeitlichen Steuerung von DA-Advertisements und -Suchanforderungen dienen.

- Wenn der SA oder UA (User Agent) statisch DA-Konfigurationsinformationen aus der `net.slp.DAAddresses`-Eigenschaft in der `slp.conf`-Datei abrufen soll, können Sie die DA-Erkennung deaktivieren.
- Wenn im Netzwerk wiederholt Partitionierungsvorgänge durchgeführt werden, können Sie die Häufigkeit von passiven Advertisements und der aktiven Erkennung ändern.
- Wenn UA- und SA-Clients auf DAs auf der anderen Seite einer Wählverbindung zugreifen, können Sie die DA-Taktfrequenz und das Intervall der aktiven Erkennung herabsetzen, um die Häufigkeit der Aktivierung einer Wählverbindung zu verringern.
- Wenn das Netzwerk stark belastet ist, können Sie das Multicasting begrenzen.

Die in diesem Abschnitt aufgeführten Verfahren beschreiben, wie die folgenden Eigenschaften modifiziert werden.

TABELLE 9–2 Eigenschaften zur zeitlichen Steuerung von DA-Advertisements und -Suchanforderungen

Eigenschaft	Beschreibung
`net.slp.passiveDADetection`	Boolescher Wert, mit dem festgelegt wird, ob `slpd` eine Überwachung von nicht angeforderten DA-Advertisements durchführt

TABELLE 9–2 Eigenschaften zur zeitlichen Steuerung von DA-Advertisements und -Suchanforderungen *(Fortsetzung)*

Eigenschaft	Beschreibung
`net.slp.DAActiveDiscoveryInterval`	Wert, mit dem festgelegt wird, wie häufig `slpd` eine aktive DA-Erkennung für einen neuen DA durchführt
`net.slp.DAHeartBeat`	Wert, mit dem festgelegt wird, wie oft ein DA ein nicht angefordertes DA-Advertisement mehrfach versendet

Beschränken von UAs und SAs auf statisch konfigurierte DAs

Es kann zuweilen erforderlich sein, UAs und SAs auf das Abrufen von DA-Adressen aus den statischen Konfigurationsinformationen in der `slp.conf`-Datei zu beschränken. Mithilfe des nächsten Verfahrens können Sie zwei Eigenschaften modifizieren, die `slpd` veranlassen, DA-Informationen ausschließlich aus der `net.slp.DAAddresses`-Eigenschaft abzurufen.

▼ So beschränken Sie UAs und SAs auf statisch konfigurierte DAs

Mithilfe des folgenden Verfahrens können Sie die `net.slp.passiveDADetection` - und die `net.slp.DAActiveDiscoveryInterval`-Eigenschaften ändern.

Hinweis – Wenden Sie dieses Verfahren nur bei Hosts an, die UAs und SAs ausführen, die auf statische Konfigurationen beschränkt sind.

---

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Setzen Sie die `net.slp.passiveDADetection`-Eigenschaft in der `slp.conf`-Datei auf `False`, um die passive Erkennung zu deaktivieren. Diese Einstellung bewirkt, dass `slpd` nicht angeforderte DA-Advertisements ignoriert.**

   ```
   net.slp.passiveDADetection=False
   ```

5 **Setzen Sie das `net.slp.DAActiveDiscoveryInterval` auf `-1`, um die anfängliche und periodische aktive Erkennung zu deaktivieren.**

```
net.slp.DAActiveDiscoveryInterval=-1
```

6 **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

7 **Starten Sie `slpd` neu, damit Ihre Änderungen wirksam werden.**

```
# svcadm enable network/slp
```

Konfigurieren der DA-Erkennung für DFÜ-Netzwerke

Wenn die UAs oder SAs durch ein DFÜ-Netzwerk vom DA getrennt sind, können Sie die DA-Erkennung konfigurieren, um Suchanforderungen und DA-Advertisements zu verringern oder zu beenden. Wenn DFÜ-Netzwerke aktiviert werden, wird normalerweise eine Gebühr erhoben. Durch das Minimieren von Aufrufen, die von außerhalb kommen, können die Kosten, die durch die Nutzung eines DFÜ-Netzwerks resultieren, gesenkt werden.

Hinweis – Mit der Methode, die unter „Beschränken von UAs und SAs auf statisch konfigurierte DAs“ auf Seite 253 beschrieben ist, können Sie die DA-Erkennung vollständig deaktivieren.

▼ So konfigurieren Sie die DA-Erkennung für DFÜ-Netzwerke

Mithilfe des folgenden Verfahrens können Sie nicht angeforderte DA-Advertisements und aktive Erkennungsvorgänge verringern, indem Sie die DA-Taktfrequenz und das Intervall der aktiven Erkennung erhöhen.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

```
# svcadm disable network/slp
```

3 **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4 **Erhöhen Sie den `net.slp.DAHeartbeat`-Eigenschaftswert in der `slpd.conf`-Datei.**

```
net.slp.DAHeartbeat=value
```

value Eine 32-Bit-Ganzzahl zur Angabe der Anzahl von Sekunden für die Taktfrequenz des passiven DA-Advertisements

Standardwert = 10800 Sekunden (3 Stunden)

Wertebereich = 2000–259200000 Sekunden

Sie können beispielsweise den DA-Takt auf einem Host, der einen DA ausführt, auf etwa 18 Stunden setzen:

```
net.slp.DAHeartbeat=65535
```

5 Erhöhen Sie den `net.slp.DAActiveDiscoveryInterval` -Eigenschaftswert in der `slpd.conf`-Datei:

```
net.slp.DAActiveDiscoveryInterval value
```

value Eine 32-Bit-Ganzzahl zur Angabe der Anzahl von Sekunden für aktive DA-Suchanforderungen

Standardwert = 900 Sekunden (15 Minuten)

Wertebereich = 300–10800 Sekunden

Sie können beispielsweise das Intervall der aktiven DA-Erkennung auf einem Host, der einen UA und einen SA ausführt, auf 18 Stunden setzen:

```
net.slp.DAActiveDiscoveryInterval=65535
```

6 Speichern Sie Ihre Änderungen und schließen Sie die Datei.

7 Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.

```
# svcadm enable network/slp
```

Konfigurieren des DA-Takts für häufige Partitionen

SAs müssen mit allen DAs registriert werden, die ihre Bereiche unterstützen. Ein DA kann erscheinen, nachdem `slpd` die aktive Erkennung durchgeführt hat. Wenn der DA die `slpd`-Bereiche unterstützt, registriert der SLP-Dämon alle Advertisements auf seinem Host mit dem DA.

Eine Möglichkeit der Erkennung von DAs durch `slpd` besteht darin, dass ein DA während des Boot-Vorgangs ein nicht angefordertes Advertisement sendet. Der SLP-Dämon verwendet das periodische nicht angeforderte Advertisement (den Takt), um zu bestimmen, ob ein DA noch aktiv ist. Wenn kein Takt vorhanden ist, entfernt der Dämon die DAs, die er selbst verwendet, sowie die DAs, die er den UAs anbietet.

Wenn ein DA im Zuge einer kontrollierten Abschaltung deaktiviert wird, sendet er ein spezielles DA-Advertisement, um die mithörenden SA-Services darüber zu informieren. Der SLP-Dämon verwendet dieses Advertisement auch dazu, um inaktive DAs aus dem Cache zu entfernen.

Wenn Ihr Netzwerk häufige Partitionen berücksichtigen muss und SAs eine lange Lebensdauer haben, kann `slpd` im Cache gespeicherte DAs während der Partitionierung entfernen, wenn keine Takt-Advertisements empfangen werden. Durch Herabsetzen der Taktfrequenz können Sie die Verzögerung verringern, bis ein deaktivierter DA im Cache wiederhergestellt wird, nachdem die Partition repariert wurde.

▼ So konfigurieren Sie den DA-Takt für häufige Partitionen

Wenden Sie das folgende Verfahren an, um die `net.slp.DAHeartBeat`-Eigenschaft zu ändern und damit die DA-Taktfrequenz zu verringern.

Hinweis – Wenn die DA-Erkennung vollständig deaktiviert ist, muss die `net.slp.DAAddresses` -Eigenschaft in `slp.conf` auf den Hosts, die UAs und SAs ausführen, deaktiviert sein, damit die Hosts auf den richtigen DA zugreifen können.

---

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Verringern Sie den `net.slp.DAHeartBeat`-Wert auf 1 Stunde (3600 Sekunden). Die DA-Taktfrequenz ist standardmäßig auf 3 Stunden (10800 Sekunden) gesetzt.**

   ```
   net.slp.DAHeartBeat=3600
   ```

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6. **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

   ```
   # svcadm enable network/slp
   ```

Entlastung des Netzwerks

Wenn das Netzwerk stark überbelastet ist, können Sie die Menge der Multicast-Vorgänge begrenzen. Wenn noch keine DAs im Netzwerk bereitgestellt sind, kann durch die Bereitstellung von DAs die Menge der SLP-bezogenen Multicast-Vorgänge verringert werden.

Multicast ist jedoch nach der Bereitstellung von DAs weiterhin für die DA-Erkennung erforderlich. Sie können die Menge der für die DA-Erkennung erforderlichen Multicast-Vorgänge verringern, indem Sie das unter „So konfigurieren Sie die DA-Erkennung für DFÜ-Netzwerke“ auf Seite 254 beschrieben Verfahren anwenden. Mithilfe der Methode, die unter „Beschränken von UAs und SAs auf statisch konfigurierte DAs“ auf Seite 253 beschrieben ist, können Sie Multicast für die DA-Ermittlung vollständig deaktivieren.

Verwenden verschiedener Netzwerkmedien, Topologien oder Konfigurationen

Die in diesem Abschnitt beschriebenen Szenarios veranschaulichen, wie Sie die folgenden Eigenschaften ändern können, um die SLP-Leistung zu optimieren.

TABELLE 9–3 SLP-Leistungseigenschaften

Eigenschaft	Beschreibung
`net.slp.DAAttributes`	Das kleinste Aktualisierungsintervall, das ein DA für Advertisements akzeptiert
`net.slp.multicastTTL`	Der für Multicast-Pakete angegebene *Lebensdauerwert* (Time-To-Live, TTL)
`net.slp.MTU`	Die Bytegröße für die Netzwerkpakete: In der Größe sind IP- und TCP- oder UDP-Header eingeschlossen.
`net.slp.isBroadcastOnly`	Der boolesche Wert, der gesetzt wird, wenn Broadcast für DA- und die nicht DA-basierte Serviceerkennung verwendet werden soll

Verringern von SA-Neuregistrierungen

SAs müssen regelmäßig ihre Service-Advertisements aktualisieren, bevor die jeweilige Lebensdauer abläuft. Wenn ein DA stark durch UAs und SAs beansprucht wird, kann er durch häufige Aktualisierungen überlastet werden. Wenn ein DA überlastet ist, werden durch UA-Anforderungen Zeitüberschreitungen ausgelöst, wonach die Anforderungen fallen gelassen werden. Zeitüberschreitungen von UA-Anforderungen können viele Ursachen haben. Bevor Sie davon ausgehen, dass das Problem aufgrund einer DA-Überlastung aufgetreten ist,

führen Sie eine snoop-Ablaufverfolgung aus, um die Lebensdauer der Service-Advertisements zu prüfen, die mit einer Serviceregistrierung registriert sind. Wenn die Lebensdauern zu kurz sind und oft Neuregistrierungen stattfinden, sind die Zeitüberschreitungen wahrscheinlich auf die häufigen Neuregistrierungen zurückzuführen.

Hinweis – Eine Serviceregistrierung ist eine *Neuregistrierung*, wenn das FRESH-Flag nicht gesetzt ist. Weitere Informationen zu Serviceregistrierungsmeldungen finden Sie in Kapitel 11, „SLP (Referenz)“.

▼ So reduzieren Sie SA-Neuregistrierungen

Wenden Sie das folgende Verfahren an, um das kleinste Aktualisierungsintervall für SAs zu erhöhen und so die Anzahl von Neuregistrierungen zu verringern.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Erhöhen Sie den Wert des `min-refresh-interval`-Attributs der `net.slp.DAAttributes`-Eigenschaft.**

   Die standardmäßige kleinste Neuregistrierungsdauer ist null. Wenn der Standardwert auf null gesetzt ist, können SAs jederzeit neu registriert werden. Im folgenden Beispiel ist das Intervall auf 3600 Sekunden (eine Stunde) gesetzt.

   ```
   net.slp.DAAttributes(min-refresh-interval=3600)
   ```

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6. **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

   ```
   # svcadm enable network/slp
   ```

Konfigurieren der Multicast-Lebensdauereigenschaft

Mit der Multicast-Lebensdauereigenschaft (`net.slp.multicastTTL`) wird der Bereich bestimmt, in dem ein Multicast-Paket in Ihrem Intranet weitergegeben wird. Die Multicast-TTL wird konfiguriert, indem die `net.slp.multicastTTL` -Eigenschaft auf einen

Ganzzahlwert zwischen 1 und 255 gesetzt wird. Der Standardwert der Multicast-TTL ist 255, was bedeutet, dass die Paketweiterleitung theoretisch nicht eingeschränkt ist. Eine TTL von 255 bewirkt jedoch, dass ein Multicast-Paket durch das Intranet bis zu den Grenzroutern am Rand Ihrer Verwaltungsdomain vordringt. Ein richtige Konfiguration von Multicast für Grenzrouter ist erforderlich, um zu verhindern, dass Multicast-Pakete in das Multicast-Backbone des Internets oder bis zu Ihrem ISP gelangen.

Die Multicast-TTL-Bereichsfestlegung ist der standardmäßigen IP-TTL ähnlich, mit der Ausnahme, dass ein TTL-Vergleich durchgeführt wird. Jeder Schnittstelle auf einem Multicast-fähigem Router wird ein TTL-Wert zugewiesen. Wenn ein Multicast-Paket ankommt, vergleicht der Router die TTL des Pakets mit der TTL der Schnittstelle. Wenn die TTL des Pakets größer als oder gleich der TTL der Schnittstelle ist, wird die Paket-TTL um eins reduziert (wie bei standardmäßiger IP-TTL). Wenn die TTL auf null reduziert wird, wird das Paket verworfen. Wenn Sie die TTL-Bereichsfestlegung für das SLP-Multicasting verwenden, müssen Ihre Router richtig konfiguriert sein, um Pakete auf einen bestimmten Unterabschnitt Ihres Intranets zu beschränken.

▼ So konfigurieren Sie die Multicast-Lebensdauereigenschaft

Anhand des folgenden Verfahrens können Sie die `net.slp.multicastTTL`-Eigenschaft zurücksetzen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.

```
# svcadm disable network/slp
```

3 Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.

4 Ändern Sie die `net.slp.multicastTTL`-Eigenschaft in der `slpd.conf`-Datei:

`net.slp.multicastTTL=`*value*

value Ein positiver Ganzzahlwert, der kleiner oder gleich 255 ist und Multicast-TTL definiert

Hinweis – Sie können den Multicast-Weitergabebereich reduzieren, indem Sie den TTL-Wert verkleinern. Wenn der TTL-Wert 1 ist, wird das Paket auf das Teilnetz beschränkt. Wenn der Wert 32 ist, wird das Paket auf den Standort beschränkt. Leider wird der Begriff *Standort* nicht durch das RFC 1075 definiert, in dem TTLs erläutert werden. Werte über 32 beziehen sich auf das theoretische Routing im Internet und sollten nicht verwendet werden. Werte unter 32 können verwendet werden, um Multicast auf eine Gruppe von zugänglichen Teilnetzen zu beschränken, wenn die Router richtig mit TTLs konfiguriert sind.

5 **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6 **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

```
# svcadm enable network/slp
```

Konfigurieren der Paketgröße

Die standardmäßige Paketgröße für SLP ist 1400 Byte. Die Größe sollte für die meisten lokalen Netzwerke ausreichen. Bei kabellosen Netzwerken oder Weitverkehrsnetzwerken können Sie die Paketgröße reduzieren, um Nachrichtenfragmentierung zu vermeiden und den Netzwerkverkehr zu verringern. Bei lokalen Netzwerken mit größeren Paketen kann die Leistung verbessert werden, indem die Paketgröße vergrößert wird. Sie können feststellen, ob die Paketgröße reduziert werden muss, indem Sie die Mindestpaketgröße für Ihr Netzwerk überprüfen. Wenn das Netzwerkmedium eine kleinere Paketgröße hat, können Sie dementsprechend den `net.slp.MTU`-Wert verkleinern.

Sie können die Paketgröße erhöhen, wenn Ihr Netzwerkmedium größere Pakete hat. Eine Änderung des `net.slp.MTU` -Werts sollte jedoch nur dann nötig sein, wenn die Service-Advertisements von SAs oder Abfragen von UAs häufig dazu führen, dass die standardmäßige Paketgröße überschritten wird. Sie können `snoop` verwenden, um festzustellen, ob die standardmäßige Paketgröße häufig aufgrund von UA-Anforderungen überschritten wird, wonach Sie im Bedarfsfall TCP anstelle von UDP verwenden.

Die `net.slp.MTU`-Eigenschaft dient zum Messen der vollständigen IP-Paketgröße einschließlich des Sicherungsschicht-Headers, des IP-Headers, des UDP- oder TCP-Headers und der SLP-Meldung.

▼ So konfigurieren Sie die Paketgröße

Anhand des folgenden Verfahrens können Sie die standardmäßige Paketgröße ändern, indem Sie die `net.slp.MTU`-Eigenschaft einstellen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Ändern Sie die `net.slp.MTU`-Eigenschaft in der `slpd.conf`-Datei:**

   `net.slp.MTU=`*value*

   value Ein 16-Bit-Ganzzahlwert zur Angabe der Netzwerkpaketgröße in Byte

   Standardwert = 1400

   Wertebereich = 128 – 8192

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6. **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

   ```
   # svcadm enable network/slp
   ```

Konfigurieren des Nur-Broadcast-Routing

SLP ist zur Verwendung von Multicast für die Serviceerkennung bei fehlenden DAs und für die DA-Erkennung bestimmt. Wenn in Ihrem Netzwerk kein Multicast-Routing verwendet wird, können Sie SLP für die Verwendung von Broadcast konfigurieren, indem Sie die `net.slp.isBroadcastOnly`-Eigenschaft auf `True` setzen.

Anders als bei Multicast werden Broadcast-Pakete nicht standardmäßig über Teilnetze weitergegeben. Aus diesem Grund funktioniert die Serviceerkennung ohne DAs nur in einem einzelnen Teilnetz. Außerdem müssen bestimmte Faktoren berücksichtigt werden, wenn DAs und Bereiche in Netzwerken bereitgestellt werden, in denen Broadcast verwendet wird. Ein DA auf einem Multihomed-Host kann die Serviceerkennung zwischen mehreren Teilnetzen übermitteln, wenn Multicast deaktiviert ist. Weitere Informationen zum Bereitstellen von DAs auf Multihomed-Hosts finden Sie unter „DA-Bereitstellung und Zuweisung von Bereichsnamen“ auf Seite 278.

▼ So konfigurieren Sie Nur-Broadcast-Routing

Wenden Sie die folgenden Verfahren an, um die `net.slp.isBroadcastOnly`-Eigenschaft auf `True` zu setzen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Setzen Sie die `net.slp.isBroadcastOnly`-Eigenschaft in der `slpd.conf`-Datei auf `True`:**

   ```
   net.slp.isBroadcastOnly=True
   ```

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6. **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

   ```
   # svcadm enable network/slp
   ```

Modifizieren von Zeitüberschreitungseinstellungen bei SLP-Suchanforderungen

In zwei Situationen kann es erforderlich sein, die Zeitüberschreitungswerte für SLP-Suchanforderungen zu ändern:

- Wenn die SLP-Agenten durch mehrere Teilnetze, Wählleitungen oder andere WANs getrennt sind, kann eine hohe Netzwerklatenz dazu führen, dass eine Anforderung oder eine Registrierung nicht durchgeführt werden kann, weil die standardmäßigen Zeitüberschreitungswerte dies nicht zulassen. Im umgekehrten Fall, d. h., wenn die Latenz Ihres Netzwerks niedrig ist, können Sie die Leistung verbessern, indem Sie die Zeitüberschreitungswerte herabsetzen.
- Wenn das Netzwerk durch starken Verkehr oder hohe Kollisionsraten belastet wird, kann die maximale Wartezeit der SAs und UAs, die verstreichen muss, bevor eine Meldung gesendet werden kann, eventuell nicht ausreichen, um kollisionsfreie Transaktionen zu gewährleisten.

Ändern der standardmäßigen Zeitüberschreitungseinstellungen

Eine hohe Netzwerklatenz kann dazu führen, dass UAs und SAs eine Zeitüberschreitung auslösen, bevor eine Antwort auf Anfragen und Registrierungen zurückgegeben wird. Die Latenz kann ein Problem sein, wenn ein UA von einem SA getrennt ist oder wenn sowohl ein UA als auch ein SA von einem DA getrennt sind – entweder durch mehrere Teilnetze, eine Wählleitung oder ein WAN. Sie können feststellen, ob die Latenz ein Problem darstellt, indem Sie überprüfen, ob fehlgeschlagene SLP-Anforderungen auf Zeitüberschreitungen bei UA- und SA-Anforderungen und Registrierungen zurückzuführen sind. Außerdem können Sie den Befehl `ping` verwenden, um die aktuelle Latenz zu messen.

In der folgenden Tabelle sind die Konfigurationseigenschaften aufgeführt, die zum Steuern der Zeitüberschreitungen dienen. Anhand der in diesem Abschnitt beschriebenen Verfahren können Sie diese Eigenschaften modifizieren.

TABELLE 9–4 Zeitüberschreitungseigenschaften

Eigenschaft	Beschreibung

`net.slp.multicastTimeouts`
`net.slp.DADiscoveryTimeouts`
`net.slp.datagramTimeouts`
	Die Eigenschaften zum Steuern von Zeitüberschreitungen für die wiederholte Übertragung von Multicast- und Unicast-UDP-Meldungen, bevor die Übertragung abgebrochen wird

`net.slp.multicastMaximumWait`	Die Eigenschaft zum Steuern der maximalen Dauer der Übertragung einer Multicast-Meldung, bevor die Übertragung abgebrochen wird
`net.slp.datagramTimeouts`	Der obere Grenzwert einer DA-Zeitüberschreitung, der durch die Summe der Werte bestimmt wird, die für diese Eigenschaft angegeben sind. Ein UDP-Datagramm wird so lange an einen DA gesendet, bis eine Antwort erfolgt oder die Zeitüberschreitungsgrenze erreicht ist.

Wenn während einer Multicast-Serviceerkennung oder einer DA-Erkennung häufige Zeitüberschreitungen stattfinden, erhöhen Sie den Wert der `net.slp.multicastMaximumWait`-Eigenschaft, deren Standardwert bei 15000 Millisekunden (15 Sekunden) liegt. Durch eine Erhöhung der maximalen Wartezeit steht mehr Zeit für Anforderungen in Netzwerken mit hoher Latenz zur Verfügung. Nachdem Sie `net.slp.multicastMaximumWait` geändert haben, sollten Sie auch `net.slp.multicastTimeouts` und `net.slp.DADiscoveryTimeouts` ändern. Die Summe der Zeitüberschreitungswerte für diese Eigenschaften entspricht dem Wert von `net.slp.multicastMaximumWait`.

▼ So ändern Sie standardmäßige Zeitüberschreitungseinstellungen

Wenden Sie das folgende Verfahren an, um die SLP-Eigenschaften zu ändern, die zum Steuern der Zeitüberschreitungsfunktion dienen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.

```
# svcadm disable network/slp
```

3 Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.

4 Ändern Sie die `net.slp.multicastMaximumWait` -Eigenschaft in der `slpd.conf`-Datei:

`net.slp.multicastMaximumWait=`*value*

value Ein 32-Bit-Ganzzahlwert zur Angabe der Summe der Werte, die für `net.slp.multicastTimeouts` und `net.slp.DADiscoveryTimeouts` gelten

Standardwert = 15000 Millisekunden (15 Sekunden)

Wertebereich = 1000 bis 60000 Millisekunden

Wenn Sie beispielsweise feststellen, dass für Multicast-Anforderungen 20 Sekunden (20000 Millisekunden) erforderlich sind, können Sie die für `net.slp.multicastTimeouts` angegebenen Werte und die `net.slp.DADiscoveryTimeouts`-Eigenschaften auf 20000 Millisekunden einstellen.

```
net.slp.multicastMaximumWait=20000
net.slp.multicastTimeouts=2000,5000,6000,7000
net.slp.DADiscoveryTimeouts=3000,3000,6000,8000
```

5 Ändern Sie nach Bedarf die `net.slp.datagramTimeouts` -Eigenschaft in der `slpd.conf`-Datei:

`net.slp.datagramTimeouts=`*value*

value Eine Liste von 32-Bit-Ganzzahlwerten, die zur Angabe von Zeitüberschreitungen in Millisekunden für die Übertragung von Unicast-Datagrammen an DAs dienen

Standardwert = 3000,3000,3000

Sie können die Datagramm-Zeitüberschreitung beispielsweise auf 20000 Millisekunden erhöhen, um häufige Zeitüberschreitungen zu vermeiden.

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

In Hochleistungsnetzwerken können Sie das Zeitüberschreitungslimit für die Übertragung von Multicast- und Unicast-UDP-Datagrammen herabsetzen. Wenn Sie das Zeitüberschreitungslimit herabsetzen, verringern Sie die Latenz, die für SLP-Anforderungen erforderlich ist.

6 **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

7 **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

```
# svcadm enable network/slp
```

Konfigurieren der Zufallswartezeit

In Netzwerken mit starkem Verkehr oder einer hohen Kollisionsrate kann die Kommunikation mit einem DA beeinträchtigt werden. Bei hohen Kollisionsraten muss der sendende Agent das UDP-Datagramm erneut übertragen. Sie können festlegen, ob eine Neuübertragung stattfindet, indem Sie `snoop` verwenden, um den Verkehr in einem Netzwerk von Hosts zu überwachen, die `slpd` als SA-Server ausführen, sowie den Verkehr auf einem Host, der `slpd` als DA ausführt. Wenn mehrere Serviceregistrierungsmeldungen für denselben Service in der `snoop`-Ablaufverfolgung des Hosts, der `slpd` als SA-Server ausführt, angezeigt werden, kann es sich um Kollisionen von Benachrichtigungen handeln.

Kollisionen können vor allem während des Boot-Vorgangs problematisch sein. Wenn ein DA gestartet wird, sendet er nicht angeforderte Advertisements, worauf die SAs mit Registrierungen antworten. SLP verlangt von den SAs, nach dem Empfang eines DA-Advertisements auf das Verstreichen einer Zufallswartezeit zu warten, bevor sie eine Antwort senden. Die Zufallswartezeit wird durch einen maximalen Wert bestimmt, der durch `net.slp.randomWaitBound` gesteuert wird. Der Standardwert der Zufallswartezeit ist 1000 Millisekunden (1 Sekunde).

▼ So konfigurieren Sie die Zufallswartezeit

Wenden Sie das folgende Verfahren an, um die `net.slp.RandomWaitBound`-Eigenschaft in der `slp.conf`-Datei zu ändern.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Ändern Sie die `net.slp.RandomWaitBound`-Eigenschaft in der `slpd.conf`-Datei:**

   `net.slp.RandomWaitBound=`*value*

   value Der obere Grenzwert zum Berechnen der Zufallswartezeit, bevor versucht wird, einen DA zu kontaktieren

   Standardwert = 1000 Millisekunden (1 Sekunde)

   Wertebereich = 1000 bis 3000 Millisekunden

   Sie können die maximale Wartezeit beispielsweise auf 2000 Millisekunden (2 Sekunden) verlängern.

   ```
   net.slp.randomWaitBound=2000
   ```

   Wenn Sie die Zufallswartezeit verlängern, findet eine längere Verzögerung der Registrierung statt. SAs können Registrierungen mit neu erkannten DAs langsamer durchführen, wodurch Kollisionen und Zeitüberschreitungen vermieden werden können.

5. **Ändern Sie nach Bedarf die `net.slp.datagramTimeouts` -Eigenschaft in der `slpd.conf`-Datei:**

   `net.slp.datgramTimeouts=`*value*

   value Eine Liste von 32-Bit-Ganzzahlwerten, die zur Angabe von Zeitüberschreitungen in Millisekunden für die Übertragung von Unicast-Datagrammen an DAs dienen

   Standardwert = 3000,3000,3000

   Sie können die Datagramm-Zeitüberschreitung beispielsweise auf 20000 Millisekunden erhöhen, um häufige Zeitüberschreitungen zu vermeiden.

   ```
   net.slp.datagramTimeouts=2000,5000,6000,7000
   ```

   In Hochleistungsnetzwerken können Sie das Zeitüberschreitungslimit für die Übertragung von Multicast- und Unicast-UDP-Datagrammen herabsetzen. Durch diese Einstellung wird die für SLP-Anforderungen erforderliche Latenz verringert.

6 **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

7 **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

```
# svcadm enable network/slp
```

Bereitstellen von Bereichen

Mithilfe von Bereichen können Sie Services bereitstellen, die von logischen, physischen und administrativen Benutzergruppen abhängig sind. Mit Bereichen können Sie den Zugriff auf Service-Advertisements kontrollieren.

Verwenden Sie die `net.slp.useScopes` -Eigenschaft, um Bereiche zu erstellen. Sie können beispielsweise in die `/etc/inet/slp.conf` -Datei auf einem Host einen neuen Bereich namens `newscope` einfügen:

```
net.slp.useScopes=newscope
```

In einen Nebenraum am Ende des Südgangs im zweiten Stock von Gebäude 6 Ihres Unternehmens stehen beispielsweise vernetzte Geräte wie etwa Drucker und Faxgeräte. Diese Geräte können von allen Mitarbeitern benutzt werden, die im zweiten Stock arbeiten. Sie können die Benutzung dieser Geräte aber auch auf die Mitarbeiter einer bestimmten Abteilung beschränken. Bereiche bieten die Möglichkeit, den Zugriff auf die Service-Advertisements für diese Geräte zu ermöglichen.

Wenn die Geräte für eine einzelne Abteilung bestimmt sind, können Sie einen Bereich mit dem Namen der betreffenden Abteilung erstellen, z. B. `mktg`. Geräte, die zu anderen Abteilungen gehören, können mit anderen Bereichsnamen konfiguriert werden.

In einem anderen Szenario können Abteilungen verteilt sein. Die Abteilungen Maschinenbau und CAD/CAM befinden sich beispielsweise auf 1. und 2. Etage. Sie können jedoch die Rechner in der zweiten Etage den Hosts auf beiden Etagen zuordnen, indem Sie die Rechner dem gleichen Bereich zuweisen. Sie können Bereiche so einrichten, dass sie die Anforderungen des Netzwerks und der Benutzer erfüllen.

Hinweis – UAs mit einem bestimmten Bereich werden nicht daran gehindert, Services zu verwenden, die in anderen Bereichen bekannt gegeben werden. Durch das Konfigurieren von Bereichen wird lediglich festgelegt, welche Service-Advertisements von einem UA ermittelt werden. Der Service dient dazu, Zugriffsbeschränkungen zu erzwingen.

Wann Bereiche zu konfigurieren sind

Für eine zweckmäßige Funktionsweise von SLP ist keine Bereichskonfiguration erforderlich. Der standardmäßige Bereich für SLP in der Solaris-Betriebsumgebung ist `default`. Wenn keine Bereiche konfiguriert sind, ist `default` der Bereich für alle SLP-Meldungen.

Sie können Bereiche in folgenden Situationen konfigurieren:

- Die von Ihnen unterstützten Organisationen wollen den Zugriff auf Service-Advertisements auf Ihre eigenen Mitarbeiter beschränken.
- Die physische Struktur der von Ihnen unterstützten Organisation erfordert, dass die Services eines bestimmten Bereichs für bestimmte Benutzer verfügbar sein müssen.
- Die Service-Advertisements, die für bestimmte Benutzer sichtbar sein sollen, müssen aufgeteilt werden.

Ein Beispiel für den ersten Fall finden Sie unter „Konfigurieren der DA-Erkennung für DFÜ-Netzwerke“ auf Seite 254. Ein Beispiel, das auf den zweiten Fall zutrifft: Eine Organisation ist auf zwei Gebäude verteilt, und den Benutzern in den Gebäuden soll der Zugriff auf die lokalen Services in den Gebäuden ermöglicht werden. Sie können die Benutzer in Gebäude 1 für den Bereich `B1` und die Benutzer in Gebäude 2 für den Bereich `B2` konfigurieren.

Überlegungen zum Konfigurieren von Bereichen

Wenn Sie die `net.slp.useScopes`-Eigenschaft in der `slpd.conf` -Datei modifizieren, konfigurieren Sie die Bereiche für alle Agenten auf dem Host. Wenn der Host SAs ausführt oder als DA fungiert, müssen Sie diese Eigenschaft konfigurieren, um die SAs oder den DA in anderen Bereichen als `default` zu konfigurieren. Wenn nur UAs auf dem Rechner ausgeführt werden und die UAs feststellen, dass SAs und DAs vorhanden sind, die andere Bereiche als `default` unterstützen, müssen Sie die Eigenschaft nicht konfigurieren, es sei denn, Sie wollen die von den UAs verwendeten Bereiche beschränken. Wenn die Eigenschaft nicht konfiguriert ist, können UAs automatisch verfügbare DAs und Bereiche über `slpd` erkennen. Der SLP-Dämon verwendet die aktive und passive DA-Erkennung, um DAs zu suchen, oder er verwendet die SA-Erkennung, wenn keine DAs ausgeführt werden. Wenn die Eigenschaft konfiguriert ist, verwenden die UAs nur die konfigurierten Bereiche und verwerfen sie nicht.

Wenn Sie vorhaben, Bereiche zu konfigurieren, sollten Sie erwägen, den `default`-Bereich in der Liste der konfigurierten Bereiche zu behalten, es sei denn, Sie sind sicher, dass die Bereiche aller im Netzwerk vorhandenen SAs konfiguriert sind. Wenn nicht konfigurierte SAs vorhanden sind, können die UAs mit konfigurierten Bereichen diese nicht finden. Dies liegt daran, dass den nicht konfigurierten SAs automatisch der `default`-Bereich zugeordnet wird, wohingegen die UAs konfigurierte Bereiche haben.

Wenn Sie zudem vorhaben, DAs mithilfe der `net.slp.DAAddresses`-Eigenschaft zu konfigurieren, vergewissern Sie sich, dass die Bereiche, die von den konfigurierten DAs unterstützt werden, dieselben sind wie die, die Sie mit der `net.slp.useScopes`-Eigenschaft konfiguriert haben. Wenn sich die Bereiche unterscheiden, gibt `slpd` eine Fehlermeldung aus, wenn er neu gestartet wird.

So konfigurieren Sie Bereiche

Wenden Sie das folgende Verfahren an, um Bereichsnamen der `net.slp.useScopes` -Eigenschaft der `slp.conf` -Datei hinzuzufügen.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

```
# svcadm disable network/slp
```

3 **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4 **Ändern Sie die `net.slp.useScopes`-Eigenschaft in der `slpd.conf`-Datei:**

`net.slp.useScopes=`<*scope names*>

scope names Eine Liste von Zeichenfolgen, die angeben, welche Bereiche ein DA oder SA für Anforderungen verwenden darf oder welche Bereiche ein DA unterstützen muss

Standardwert = Standard für SA und DA/nicht zugewiesen für UA

Hinweis –

Verwenden Sie Folgendes, um Bereichsnamen zu konstruieren:

- Alphanumerische Zeichen, Groß- oder Kleinbuchstaben
- Interpunktionszeichen (außer ″, \, *!*, <, =, > und ~)
- Leerzeichen als Teil des Namens
- Nicht-ASCII-Zeichen

  Sie können einen umgekehrten Schrägstrich als Codewechselzeichen für Nicht-ASCII-Zeichen verwenden. Für die UTF-8-Codierung wird beispielsweise der `0xc3a9`-Hexadezimalcode verwendet, um den Buchstaben *e* mit einem Accent *aigue*

darzustellen. Wenn die Plattform UTF-8 nicht unterstützt, verwenden Sie den UTF-8-Hexadezimalcode als Escape-Zeichenfolge `\c3\a9`.

Um beispielsweise Bereiche für die `eng`- und `mktg` -Gruppe in `bldg6` anzugeben, ändern Sie die `net.slp.useScopes` -Zeile wie folgt:

```
net.slp.useScopes=eng,mktg,bldg6
```

5 **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6 **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

```
# svcadm enable network/slp
```

Bereitstellen von DAs

In diesem Abschnitt wird die strategische Bereitstellung von DAs in einem Netzwerk beschrieben, in dem SLP ausgeführt wird.

SLP funktioniert nur in Verbindung mit den Basisagenten (UAs und SAs), aber nicht in Verbindung mit bereitgestellten DAs oder konfigurierten Bereichen. Alle Agenten, die keine spezielle Konfiguration aufweisen, verwenden den `default`-Bereich. DAs dienen als Cache für Service-Advertisements. Durch die Bereitstellung von DAs wird die Anzahl von Meldungen verringert, die über das Netzwerk übermittelt werden. Außerdem wird die Zeit reduziert, die erforderlich ist, um Antworten auf die Meldungen zu erhalten. Diese Funktion ermöglicht SLP, größere Netzwerke aufzunehmen.

Welchem Zweck dient die Bereitstellung eines SLP-DA?

Der Hauptgrund für die Bereitstellung von DAs ist die Verringerung des Multicast-Datenverkehrs und der Verzögerungen, die mit der Erfassung von Unicast-Antworten verbunden sind. In einem großen Netzwerk mit vielen UAs und SAs kann der mit der Serviceerkennung verbundene Multicast-Datenverkehr so stark zunehmen, dass das Netzwerk an Leistungsfähigkeit verliert. Durch Bereitstellen eines oder mehrerer DAs müssen UAs einzelne Serviceanforderungen an DAs senden, und SAs müssen sich mit DAs mithilfe von Unicast registrieren. Das einzige SLP-registrierte Multicast in einem Netzwerk mit DAs ist für die aktive und passive DA-Erkennung bestimmt.

SAs werden automatisch mit DAs registriert, die innerhalb der gemeinsamen Bereiche erkannt werden, sodass keine Multicast-Serviceanforderungen akzeptiert werden müssen. Multicast-Anforderungen in Bereichen, die nicht vom DA unterstützt werden, werden jedoch weiterhin vom SA beantwortet.

Serviceanforderungen von UAs werden einzeln an DAs versendet, anstatt diese mehrfach im Netzwerk zu versenden, wenn ein DA in den Bereichen des UA bereitgestellt ist. Dementsprechend wird das Multicast durch DAs in den Bereichen des UA reduziert. Wenn das Multicast für normale UA-Anforderungen entfällt, wird die Zeit, die für den Empfang von Antworten benötigt wird, bedeutend reduziert (von Sekunden auf Millisekunden).

DAs sind der Mittelpunkt für SA- und UA-Aktivitäten. Durch Bereitstellen eines oder mehrerer DAs für eine Reihe von Bereichen entsteht ein zentraler Punkt für die Überwachung der SLP-Aktivität. Durch die Verwendung der DA-Protokollierung ist es einfacher, Registrierungen und Anforderungen zu überwachen, als die Protokolle von mehreren im Netzwerk verstreuten SAs zu überprüfen. Sie können je nach zu bewältigenden Rechenlasten beliebig viele DAs für einen bestimmten Bereich oder mehrere Bereiche bereitstellen.

In Netzwerken ohne aktiviertes Multicast-Routing können Sie SLP für die Verwendung von Broadcast verwenden. Broadcasts sind jedoch sehr ineffizient, weil jeder Host die Meldung verarbeiten muss. Außerdem werden Broadcasts normalerweise nicht über Router weitergegeben. Dadurch können Services in einem Netzwerk ohne Multicast-Routing-Unterstützung nur im selben Teilnetz erkannt werden. Eine teilweise Unterstützung des Multicast-Routing führt dazu, dass die Erkennung von Services in einem Netzwerk inkonsistent ist. Multicast-Meldungen werden für die Erkennung von DAs verwendet. Eine teilweise Unterstützung des Multicast-Routing hat darum zur Folge, dass UAs und SAs die Services mit allen bekannten DAs im Bereich des SA registrieren. Wenn beispielsweise ein UA einen DA namens `DA1` abfragt und der SA Services mit `DA2` registriert hat, kann der UA keinen Service erkennen. Weitere Informationen zum Bereitstellen von SLP in Netzwerken ohne Multicast finden Sie unter „Konfigurieren des Nur-Broadcast-Routing“ auf Seite 261.

Bei einem Netzwerk mit inkonsistenter standortübergreifender Unterstützung des Multicast-Routing müssen Sie die SLP-UAs und SAs mit einer konsistenten Liste von DA-Standorten konfigurieren, indem Sie die `net.slp.DAAdresseses`-Eigenschaft verwenden.

Der SLPv2-DA von unterstützt auch die Interoperabilität mit SLPv1. Die SLPv1-Interoperabilität ist standardmäßig im DA aktiviert. Wenn in Ihrem Netzwerk SLPv1-Geräte (wie beispielsweise Drucker) enthalten sind oder Sie die Software Novell Netware 5 einsetzen, die SLPv1 für die Serviceerkennung verwendet, sollten Sie einen DA bereitstellen. Ohne einen DA sind die Solaris-SLP-UAs nicht in der Lage, von SLPv1 bekannt gegebene Services zu finden.

Wann DAs bereitzustellen sind

Stellen Sie DAs in Ihrem Unternehmen bereit, wenn eine der folgenden Bedingungen zutrifft:

- Bei einer Messung mit `snoop` wurde festgestellt, dass der Multicast-SLP-Datenverkehr 1 Prozent der Bandbreite in Ihrem Netzwerk übersteigt.
- Die UA-Clients müssen lange Verzögerungen oder Zeitüberschreitungen während der Anforderung von Multicast-Services in Kauf nehmen.
- Sie haben vor, die Überwachung der SLP-Service-Advertisements für bestimmte Bereiche auf einem oder mehreren Hosts zu zentralisieren.
- Ihr Netzwerk ist nicht Multicast-fähig und besteht aus mehreren Teilnetzen, die Services gemeinsam nutzen.
- In Ihrem Netzwerk werden Geräte eingesetzt, die frühere Versionen von SLP (SLPv1) unterstützen, oder Sie planen, die SLP-Serviceerkennung in Verbindung mit Novell Netware 5 einzusetzen.

▼ So stellen Sie DAs bereit

Wenden Sie das folgende Verfahren, an um die `net.slp.isDA`-Eigenschaft in der `slp.conf`-Datei auf `True` zu setzen.

Hinweis – Sie können nur einen DA pro Host zuweisen.

---

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Setzen Sie die `net.slp.isDA`-Eigenschaft in der `slpd.conf`-Datei auf `True`:**

   ```
   net.slp.isDA=True
   ```

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6 **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

```
# svcadm enable network/slp
```

Wo DAs bereitzustellen sind

Dieser Abschnitt enthält Empfehlungen, wo DAs in verschiedenen Situationen bereitzustellen sind:

- Wenn das Multicast-Routing nicht aktiviert ist und DAs benötigt werden, um die Serviceerkennung zwischen Teilnetzen zu ermöglichen

  In diesem Fall muss ein DA auf einem Host mit Schnittstellen und allen Teilnetzen bereitgestellt werden, die Services gemeinsam nutzen. Die `net.slp.interfaces`-Konfigurationseigenschaft muss *nicht* definiert werden, es sei denn, IP-Pakete werden nicht zwischen den Schnittstellen weitergeleitet. Weitere Informationen zum Konfigurieren der `net.slp.interfaces`-Eigenschaft finden Sie unter „Multihoming-Konfiguration für SLP“ auf Seite 274.
- Wenn DAs für die Skalierbarkeit bereitgestellt werden und dadurch in erster Linie der Agentenzugriff optimiert werden soll

  UAs geben normalerweise viele Serviceanforderungen an DAs weiter. Ein SA registriert sich einmal mit einem DA und kann das Advertisement in periodischen, aber seltenen Intervallen aktualisieren. Dementsprechend erfolgt der UA-Zugriff auf DAs sehr viel häufiger als der SA-Zugriff. Auch ist die Zahl der Service-Advertisements normalerweise kleiner als die Zahl der Anforderungen. Darum lassen sich die meisten DA-Bereitstellungen effizienter gestalten, wenn sie für den UA-Zugriff optimiert werden.
- Bereitstellen von DAs, sodass sie sich topologisch nahe bei den UAs im Netzwerk befinden, wodurch der UA-Zugriff optimiert wird

  Natürlich müssen Sie den DA mit einem Bereich konfigurieren, der sowohl von den UA-Clients als auch von den SA-Clients genutzt wird.

Bereitstellen von mehreren DAs für den Lastausgleich

Sie können mehrere DAs für dieselbe Gruppe von Bereichen zwecks Lastausgleich bereitstellen. Stellen Sie DAs in folgenden Fällen bereit:

- UA-Anforderungen an einen DA lösen eine Zeitüberschreitung aus oder werden mit der Fehlermeldung `DA_BUSY_NOW` zurückgegeben.
- Das DA-Protokoll zeigt, dass viele SLP-Anforderungen fallen gelassen werden.
- Das Netzwerk der Benutzer, die gemeinsam die Services in den Bereichen nutzen, umspannt eine Reihe von Gebäuden oder physischen Standorten.

Sie können eine `snoop`-Ablaufverfolgung des SLP-Datenverkehrs durchführen, um festzustellen, wie viele UA-Anforderungen mit der Fehlermeldung `DA_BUSY_NOW` zurückgegeben werden. Wenn sehr viele UA-Anforderungen zurückgegeben werden, können UAs in Gebäuden, die physisch und topologisch vom DA entfernt sind, langsam antworten oder übermäßig viele Zeitüberschreitungen auslösen. In solch einem Fall können Sie in jedem Gebäude einen DA bereitstellen, um die Reaktionsfähigkeit der UA-Clients innerhalb des Gebäudes zu verbessern.

Leitungsverbindungen zwischen Gebäuden sind oft langsamer als lokale Netzwerke innerhalb von Gebäuden. Wenn Ihr Netzwerk mehrere Gebäude oder physische Standorte umspannt, setzen Sie die `net.slp.DAAddresses`-Eigenschaft in der `/etc/inet/slp.conf`-Datei auf eine Liste von spezifischen Hostnamen oder -adressen, damit die UAs nur auf die von Ihnen angegebenen DAs zugreifen.

Wenn ein bestimmter DA viel Hostspeicher für Serviceregistrierungen belegt, verringern Sie die Anzahl der SA-Registrierungen, indem Sie die Anzahl der Bereiche reduzieren, die vom DA unterstützt werden. Sie können einen Bereich, der viele Registrierungen aufweist, in zwei Teile aufteilen. Dann können Sie einen der neuen Bereiche unterstützen, indem Sie einen weiteren DA auf einem anderen Host bereitstellen.

SLP und Multihoming

Ein Multihomed-Server fungiert als Host in mehreren Teilnetzen. Der Server kann mehrere Netzwerkschnittstellenkarten haben und als Router fungieren. IP-Pakete, zu denen auch Multicast-Pakete zählen, werden über Schnittstellen weitergeleitet. In manchen Fällen wird das Routing zwischen Schnittstellen deaktiviert. In den folgenden Abschnitten wird beschrieben, wie SLP in solchen Fällen konfiguriert wird.

Multihoming-Konfiguration für SLP

Wenn keine Konfiguration durchgeführt wurde, überwacht `slpd` die Multicast- und UDP/TCP-Unicast-Sendungen an der standardmäßigen Netzwerkschnittstelle. Wenn Unicast- und Multicast-Routing zwischen den Schnittstellen eines Multihomed-Rechners aktiviert ist, ist keine zusätzliche Konfiguration erforderlich. Dies ist darauf zurückzuführen, dass Multicast-Pakete, die an einer anderen Schnittstelle ankommen, ordnungsgemäß zum standardmäßigen Ziel weitergeleitet werden. Aus diesem Grund treffen Multicast-Anforderungen, bei denen es sich um den DA oder andere Service-Advertisements handelt, bei `slpd` ein. Wenn das Routing aus irgendeinem Grund nicht aktiviert ist, wird eine Konfiguration angefordert.

Wann mehrere nicht gesteuerte Netzwerkschnittstellen zu konfigurieren sind

Wenn einer der folgenden Fälle auftritt, müssen Sie eventuell Multihomed-Rechner konfigurieren.

- Das Unicast-Routing zwischen den Schnittstellen ist aktiviert und das Multicast-Routing ist deaktiviert.
- Sowohl das Unicast-Routing als auch das Multicast-Routing sind zwischen den Schnittstellen deaktiviert.

Wenn das Multicast-Routing zwischen den Schnittstellen deaktiviert ist, ist dies normalerweise darauf zurückzuführen, dass Multicast nicht im Netzwerk bereitgestellt wurde. In diesem Fall wird Broadcast normalerweise für die nicht DA-basierte Serviceerkennung und für die DA-Erkennung in einzelnen Teilnetzen verwendet. Broadcast wird konfiguriert, indem die `net.slp.isBroadcastOnly` -Eigenschaft auf `True` gesetzt wird.

Konfigurieren mehrerer nicht gesteuerter Netzwerkschnittstellen (Übersicht der Schritte)

TABELLE 9–5 Konfigurieren mehrerer nicht gesteuerter Netzwerkschnittstellen

Aufgabe	Beschreibung	Siehe
Konfigurieren der `net.slp.interfaces`-Eigenschaft	Legen Sie diese Eigenschaft fest, damit `slpd` die Unicast- und Multicast-/Broadcast-SLP-Anforderungen an bestimmten Schnittstellen überwachen kann.	„Konfigurieren der `net.slp.interfaces`-Eigenschaft“ auf Seite 276
Einrichten der Proxyservice-Advertisements, damit UAs in Teilnetzen Service-URLs mit erreichbaren Adressen erhalten	Beschränken Sie das Proxy-Advertisement auf einen Rechner, auf dem `slpd` ausgeführt wird, der mit einem einzelnen Teilnetz anstelle eines Multihomed-Hosts verbunden ist.	„Proxy-Advertisement auf Multihomed-Hosts“ auf Seite 277
Bereitstellen der DAs und Konfigurieren von Bereichen, um die Erreichbarkeit zwischen UAs und SAs zu gewährleisten	Konfigurieren Sie die `net.slp.interfaces`-Eigenschaft auf Multihomed-Hosts mit einem einzelnen Schnittstellen-Hostnamen oder einer einzelnen Adresse. Führen Sie einen DA auf einem Multihomed-Host aus, aber konfigurieren Sie Bereiche, damit die SAs und UAs in jedem Teilnetz verschiedene Hosts verwenden.	„DA-Bereitstellung und Zuweisung von Bereichsnamen“ auf Seite 278

Konfigurieren der `net.slp.interfaces`-Eigenschaft

Wenn die `net.slp.interfaces` -Eigenschaft definiert ist, überwacht `slpd` die Unicast- und Multicast-/Broadcast-SLP-Anforderungen an den in der Eigenschaft angegebenen Schnittstellen, nicht aber an der standardmäßigen Schnittstelle.

Normalerweise definieren Sie die `net.slp.interfaces` -Eigenschaft in Verbindung mit der Aktivierung von Broadcast, indem Sie die `net.slp.isBroadcastOnly`-Eigenschaft festlegen, weil Multicast nicht im Netzwerk bereitgestellt wurde. Falls Multicast zwar bereitgestellt, aber nicht auf dem betreffenden Multihomed-Host gesteuert wird, kann eine Multicast-Anforderung von mehreren Schnittstellen bei `slpd` ankommen. Dies geschieht, wenn das Routing der Pakete von einem anderen Multihomed-Host oder Router durchgeführt wird, der die Teilnetze verbindet, die von den Schnittstellen bedient werden.

In einer solchen Situation erhält der SA-Server oder der UA, der die Anforderung sendet, zwei Antworten von `slpd` auf dem Multihomed-Host. Die Antworten werden dann von den Clientbibliotheken gefiltert und sind für den Client nicht sichtbar. Die Antworten sind jedoch in der `snoop`-Ablaufverfolgung sichtbar.

Hinweis –

Wenn das Unicast-Routing deaktiviert ist, sind die Services, die von den SA-Clients auf den Multihomed-Hosts bekannt gegeben werden, möglicherweise nicht von allen Teilnetzen aus erreichbar. Wenn Services nicht erreichbar sind, können die SA-Clients folgende Schritte ausführen:

- Eine Service-URL für jedes Teilnetz bekannt geben
- Sicherstellen, dass Anforderungen aus einem bestimmten Teilnetz mit einer erreichbaren URL beantwortet werden

---

Die SA-Clientbibliothek unternimmt keine Schritte, um sicherzustellen, dass erreichbare URLs bekannt gegeben werden. Das Serviceprogramm, das einen Multihomed-Host ohne Routing verarbeiten oder auch nicht verarbeiten kann, muss dann gewährleisten, dass erreichbare URLs bekannt gegeben werden.

Bevor Sie einen Service auf einem Multihomed-Host mit deaktiviertem Unicast-Routing bereitstellen, verwenden Sie `snoop` um festzustellen, ob der Service die Anforderungen von mehreren Teilnetzen richtig verarbeitet. Wenn Sie vorhaben, einen DA auf einem Multihomed-Host bereitzustellen, informieren Sie sich unter „DA-Bereitstellung und Zuweisung von Bereichsnamen“ auf Seite 278.

▼ So konfigurieren Sie die `net.slp.interfaces` -Eigenschaft

Wenden Sie das folgende Verfahren an, um die `net.slp.interfaces`-Eigenschaft in der `slp.conf`-Datei zu ändern.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

3. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

4. **Ändern Sie die `net.slp.interfaces`-Eigenschaft in der `slpd.conf`-Datei:**

   `net.slp.interfaces=`*value*

   value Liste von IPv4-Adressen oder Hostnamen der Netzwerkschnittstellenkarten, die vom DA oder SA auf Multicast-, Unicast-UDP- und TCP-Meldungen an Port 427 überwacht werden sollen

   Ein deaktivierter Server mit drei Netzwerkkarten und Multicast-Routing ist beispielsweise mit drei Teilnetzen verbunden. Die IP-Adressen der drei Netzwerkschnittstellen sind `192.147.142.42`, `192.147.143.42` und `192.147.144.42`. Die Teilnetzmaske ist `255.255.255.0` . Die folgenden Eigenschaftseinstellungen bewirken, dass `slpd` an allen drei Schnittstellen Unicast- und Multicast-/Broadcast-Nachrichten überwacht:

   ```
   net.slp.interfaces=192.147.142.42,192.147.143.42,192.147.144.42
   ```

   Hinweis – Sie können IP-Adressen oder auflösbare Hostnamen für die `net.slp.interfaces`-Eigenschaft angeben.

5. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

6. **Starten Sie `slpd` neu, um Ihre Änderungen zu aktivieren.**

   ```
   # svcadm enable network/slp
   ```

Proxy-Advertisement auf Multihomed-Hosts

Wenn ein Host mit mehreren Schnittstellen Services mithilfe von `slpd` und der Proxyregistrierung bekannt gibt, müssen die Service-URLs, die von `slpd` bekannt gegeben

werden, erreichbare Hostnamen oder Adressen enthalten. Wenn das Unicast-Routing zwischen den Schnittstellen aktiviert ist, können die Hosts in allen Teilnetzen die Hosts in anderen Teilnetzen erreichen. Proxyregistrierungen können auch für einen Service in einem Teilnetz durchgeführt werden. Wenn das Unicast-Routing jedoch deaktiviert ist, können die Serviceclients in einem Teilnetz nicht über den Multihomed-Host die Services in einem anderen Teilnetz erreichen. Diese Clients können jedoch die Services über einen anderen Router erreichen.

Ein Host mit dem standardmäßigen Hostnamen `bigguy` hat beispielsweise drei Schnittstellenkarten in drei verschiedenen nicht gesteuerten Teilnetzen. Die Hostnamen in diesen Teilnetzen sind`bigguy`, mit der IP-Adresse `192.147.142.42` , `bigguy1`, mit der IP-Adresse `192.147.143.42` und `bigguy2`, mit der IP-Adresse `192.147.144.42`. Ein alter Drucker, `oldprinter`, ist beispielsweise mit dem Teilnetz `143` verbunden und die URL `service:printing:lpr://oldprinter/queue1` ist mit `net.slp.interfaces` konfiguriert, wodurch alle Schnittstellen überwacht werden. Die `oldprinter`-URL wird vom Proxy an allen Schnittstellen bekannt gegeben. Die Rechner in den Teilnetzen `142` und `144` erhalten die URL als Antwort auf Serviceanforderungen, können aber nicht auf den `oldprinter`-Service zugreifen.

Die Lösung dieses Problems besteht darin, das Proxy-Advertisement mit `slpd` durchzuführen, der auf dem Rechner ausgeführt wird, der nur mit dem Teilnetz `143` verbunden ist, wodurch der Multihomed-Host nicht verwendet wird. Nur die Hosts im Teilnetz `143` können das Advertisement als Antwort auf eine Serviceanforderung erhalten.

DA-Bereitstellung und Zuweisung von Bereichsnamen

Die Bereitstellung von DAs und die Zuweisung von Bereichsnamen in einem Netzwerk mit einem Multihomed-Host muss mit Bedacht durchgeführt werden, um sicherzustellen, dass Clients die verfügbaren Services abrufen können. Seien Sie besonders vorsichtig, wenn das Routing deaktiviert und die `net.slp.interfaces`-Eigenschaft konfiguriert ist. Es sei nochmals darauf hingewiesen, dass keine zusätzliche DA- und Bereichskonfiguration erforderlich ist, wenn Unicast-Routing zwischen den Schnittstellen eines Multihomed-Rechners aktiviert ist. Die Advertisements werden zusammen mit den DA-Erkennungsservices zwischengespeichert, auf die über jedes Teilnetz zugegriffen werden kann. Wenn das Unicast-Routing jedoch deaktiviert ist, kann eine unzureichende Bereitstellung von DAs zu Problemen führen.

Um sich eine Vorstellung von den Problemen zu machen, die aus der Konstellation des vorangegangenen Beispiels resultieren können, sollten Sie sich vor Augen führen, was geschehen würde, wenn `bigguy` einen DA ausführt und die Clients in allen Teilnetzen dieselben Bereiche haben. SAs im Teilnetz `143` registrieren ihre Service-Advertisements mit dem DA. UAs im Teilnetz `144` können diese Service-Advertisements abrufen, obwohl die Hosts im Teilnetz `143` nicht erreichbar sind.

Eine Lösung für dieses Problem besteht darin, einen DA in jedem Teilnetz und nicht auf dem Multihomed-Host auszuführen. In diesem Fall sollte die `net.slp.interfaces`-Eigenschaft auf den Multihomed-Hosts mit einem einzelnen Schnittstellen-Hostnamen oder einer einzelnen Schnittstellenadresse konfiguriert werden oder nicht konfiguriert belassen werden, wodurch die Verwendung der standardmäßigen Schnittstelle erzwungen wird. Der Nachteil dieser Lösung besteht darin, dass Multihomed-Hosts oft größere Rechner sind, die sich besser zur Bewältigung der Rechenlast eines DA eignen.

Eine weitere Lösung besteht darin, einen DA auf dem Multihomed-Host auszuführen, aber Bereiche zu konfigurieren, wodurch die SAs und UAs in jedem Teilnetz einen anderen Bereich haben. Im vorangegangenen Beispiel können die UAs und SAs im Teilnetz `142` einen Bereich namens `scope142` haben. Die UAs und SAs im Teilnetz `143` können einen anderen Bereich namens `scope143` haben und die UAs und SAs im Teilnetz `144` können einen dritten Bereich namens `scope144` haben. Sie können die `net.slp.interfaces`-Eigenschaft auf `bigguy` mit den drei Schnittstellen konfigurieren, sodass der DA drei Bereiche in drei Teilnetzen bedient.

Überlegungen zum Konfigurieren von mehreren nicht gesteuerten Netzwerkschnittstellen

Durch das Konfigurieren der `net.slp.interfaces` -Eigenschaft wird einem DA auf dem Multihomed-Host ermöglicht, Service-Advertisements zwischen Teilnetzen zu übermitteln. Eine solche Konfiguration ist sinnvoll, wenn das Multicast-Routing im Netzwerk deaktiviert ist, während das Unicast-Routing zwischen den Schnittstellen auf einem Multihomed-Host aktiviert ist. Da Unicast zwischen den Schnittstellen gesteuert wird, können die Hosts, die sich nicht im gleichen Teilnetz wie der Service befinden, den Service kontaktieren, sobald sie die Service-URL erhalten. Ohne den DA erhalten die zu einem Teilnetz gehörenden SA-Server nur die Broadcast-Sendungen aus demselben Teilnetz, wodurch sie keine Services lokalisieren können, die sich außerhalb ihres Teilnetzes befinden.

Der häufigste Grund, warum die `net.slp.interfaces` -Eigenschaft nicht konfiguriert werden muss, ist, dass Multicast nicht bereitgestellt ist und stattdessen Broadcast verwendet wird. In anderen Fällen gilt es, umfassende Vorüberlegungen anzustellen und sorgfältig zu planen, um unnötige doppelte Antworten oder die Nichterreichbarkeit von Services zu vermeiden.

◆ ◆ ◆ KAPITEL 10

10 Integrieren von veralteten Services

Veraltete Services sind Netzwerkdienste, die aus der Zeit der Entwicklung und Implementierung von SLP stammen. Services wie der Zeilendrucker-Dämon (`lpsched`), der NFS-Dateiservice und der NIS/NIS+-Name Service enthalten beispielsweise keine internen SAs für SLP. In diesem Kapitel wird beschrieben, wann und wie veraltete Services bekannt zu geben sind.

- „Wann veraltete Services bekannt zu geben sind“ auf Seite 281
- „Advertisement von veralteten Services“ auf Seite 281
- „Überlegungen zum Advertisement von veralteten Services“ auf Seite 286

Wann veraltete Services bekannt zu geben sind

Durch das Advertisement von veralteten Services können die SLP-UAs die im Folgenden beschrieben Geräte und Services in Ihren Netzwerken suchen. Es kann nach Hardware und Software-Services gesucht werden, die keine SLP-SAs enthalten. Wenn Anwendungen mit SLP-UAs Drucker oder Datenbanken suchen müssen, die keine SLP-SAs enthalten, kann das Advertisement von veralteten Services erforderlich sein.

Advertisement von veralteten Services

Wenden Sie eine der folgenden Methoden an, um veraltete Services bekannt zu geben:

- Modifizieren des Service, um einen SLP-SA zu integrieren
- Schreiben eines kleinen Programms, dass das Advertisement anstelle eines nicht SLP-fähigen Service ausführt
- Verwenden Sie das Proxy-Advertisement, um den Service durch `slpd` bekannt geben zu lassen.

Modifizieren des Service

Wenn der Quellcode für den Softwareserver zur Verfügung steht, können Sie einen SLP-SA integrieren. Die C- und Java-APIs für SLP sind relativ einfach in der Anwendung. Informationen zur C-API finden Sie auf den entsprechenden Manpages, und Informationen zur Java-API finden Sie in der entsprechenden Dokumentation. Wenn der Service ein Hardwaregerät ist, ist beim Hersteller eventuell ein aktualisierter PROM mit integriertem SLP erhältlich. Weitere Informationen erhalten Sie vom Hersteller des Geräts.

Bekanntgeben eines Service, der nicht SLP-fähig ist

Wenn weder der Quellcode noch ein aktualisierter PROM mit SLP zur Verfügung steht, können Sie ein kleines Programm schreiben, das die SLP-Clientbibliothek zwecks Advertisement des Service verwendet. Dieses Programm kann als kleiner Dämon fungieren, den Sie über das gleiche Shell-Skript starten und stoppen können, das Sie verwenden, um den Service zu starten und zu stoppen.

SLP-Proxyregistrierung

Solaris-`slpd` unterstützt das Advertisement von veralteten Services mit einer Proxyregistrierungsdatei. Bei der Proxyregistrierungsdatei handelt es sich um eine Liste von Service-Advertisements in einem übertragbaren Format.

▼ So aktivieren Sie die SLP-Proxyregistrierung

1. **Erstellen Sie eine Proxyregistrierungsdatei auf dem Host-Dateisystem oder in einem Netzwerkverzeichnis, auf das über HTTP zugegriffen werden kann.**

2. **Stellen Sie fest, ob eine Servicetypvorlage für den Service vorhanden ist.**

   Die Vorlage ist eine Beschreibung der Service-URL und der Attribute eines Servicetyps. Eine Vorlage wird verwendet, um die Komponenten eines Advertisement für einen bestimmten Servicetyp zu definieren:

   - Wenn eine Servicetypvorlage vorhanden ist, verwenden Sie die Vorlage, um die Proxyregistrierung aufzubauen. Weitere Informationen zu Servicetypvorlagen finden Sie in RFC 2609.
   - Wenn keine Servicetypvorlage für den Service zur Verfügung steht, verwenden Sie eine Gruppe von Attributen, um den Service genau zu beschreiben. Verwenden Sie nicht die standardmäßig für das Advertisement definierte Naming-Berechtigung. Die standardmäßige Naming-Berechtigung ist nur bei standardisierten Servicetypen zugelassen. Weitere Informationen zu Naming-Berechtigungen finden Sie in RFC 2609.

Ein Unternehmen namens *BizApp* setzt beispielsweise ein lokale Datenbank ein, um Softwarefehler zu verfolgen. Um die Datenbank bekannt zu geben, kann das Unternehmen eine URL mit dem Servicetyp `service:bugdb.bizapp` verwenden. Die Naming-Berechtigung ist dann `bizapp`.

3. **Führen Sie die nächsten Schritte aus, um die `net.slp.serializedRegURL` -Eigenschaft in der `/etc/inet/slp.conf`-Datei unter Verwendung des Speicherorts der Registrierungsdatei zu konfigurieren, die in den vorangegangenen Schritten erstellt wurde.**

4. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

5. **Stoppen Sie `slpd` und alle SLP-Aktivitäten auf dem Host.**

   ```
   # svcadm disable network/slp
   ```

6. **Sichern Sie die standardmäßige `/etc/inet/slp.conf`-Datei, bevor Sie die Konfigurationseinstellungen ändern.**

7. **Geben Sie den Speicherort der Proxyregistrierungsdatei in der `net.slp.serializedRegURL`-Eigenschaft der `/etc/inet/slp.conf`-Datei an.**

   `net.slp.net.slp.serializedRegURL=`*proxy registration file URL*

   Wenn es sich bei der serialisierten Registrierungsdatei beispielsweise um `/net/inet/slp.reg` handelt, konfigurieren Sie die Eigenschaft wie folgt:

   ```
   net.slp.serializedRegURL=file:/etc/inet/slp.reg
   ```

8. **Speichern Sie Ihre Änderungen und schließen Sie die Datei.**

9. **Starten Sie `slpd` neu, damit Ihre Änderungen wirksam werden.**

   ```
   # svcadm enable network/slp
   ```

Verwenden der SLP-Proxyregistrierung für das Advertisement

Ein Service-Advertisement besteht aus Zeilen zur Angabe der Service-URL, einem optionalen Bereich und einer Reihe von Attributdefinitionen. Der SLP-Dämon liest, registriert und verwaltet Proxy-Advertisements genau so, wie es bei einem SA-Client der Fall sein würde. Es folgt ein Beispiel für ein Advertisement durch eine Proxyregistrierungsdatei.

In dem Beispiel werden ein vorhandener Drucker, der das LPR-Protokoll unterstützt, und ein FTP-Server bekannt gegeben. Die zu Beschreibungszwecken hinzugefügten Zeilennummern gehören nicht zur Datei.

```
(1) #Advertise legacy printer.
(2)
(3) service:lpr://bizserver/mainspool,en,65535
(4) scope=eng,corp
(5) make-model=Laserwriter II
(6) location-description=B16-2345
(7) color-supported=monochromatic
(8) fonts-supported=Courier,Times,Helvetica 9 10
(9)
(10) #Advertise FTP server
(11)
(12) ftp://archive/usr/src/public,en,65535,src-server
(13) content=Source code for projects
(14)
```

Hinweis – Die Proxyregistrierungsdatei unterstützt dieselben Konventionen für die Unterbrechung von Nicht-ASCII-Zeichen wie die Konfigurationsdatei. Weitere Informationen zum Format der Proxyregistrierungsdatei finden Sie in RFC 2614.

TABELLE 10–1 Beschreibung der SLP-Proxyregistrierungsdatei

Zeilennummern	Beschreibung
1 und 10	Kommentarzeilen beginnen mit einem Nummernzeichen (#) und haben keinee Auswirkungen auf die Funktion der Datei. Alle Zeichen bis zum Ende einer Kommentarzeile werden ignoriert.
2, 9 und 14	Leere Zeilen zur Begrenzung der Advertisements

TABELLE 10–1 Beschreibung der SLP-Proxyregistrierungsdatei *(Fortsetzung)*

Zeilennummern	Beschreibung
3 und 12	Service-URLs mit je drei erforderlichen Feldern und einem optionalen Feld, die durch Kommas getrennt werden: ■ Generisch oder durch `service: URL` bekannt gegeben. Informationen zur Bildung einer service:-URL finden Sie in RFC 2609. ■ Sprache des Advertisements. Im vorangegangenen Beispiel ist im Feld Englisch (*en*) festgelegt. Die Sprache wird in Form eines RFC 1766-Sprachcodes angegeben. ■ Lebensdauer der Registrierung, gemessen in Sekunden. Die Lebensdauer ist auf einen 16-Bit-Ganzzahlwert ohne Vorzeichen beschränkt. Wenn die Lebensdauer kleiner als das Maximum (65535) ist, löst `slpd` eine Zeitüberschreitung für das Advertisement aus. Wenn die Lebensdauer 65535 beträgt, aktualisiert `slpd` das Advertisement periodisch, und die Lebensdauer wird als dauerhaft betrachtet, bis `slpd` beendet wird. ■ (Optional) Diensttypfeld – Dieses Feld dient zum Definieren des Servicetyps. Wenn die Service-URL definiert ist, können Sie den Servicetyp ändern, unter dem die URL bekannt gegeben wird. Im vorangegangenen Beispiel für eine Proxyregistrierungsdatei enthält Zeile 12 eine generische FTP-URL. Das optionale Typfeld bewirkt, dass die URL unter dem Servicetypnamen *src-server* bekannt gegeben wird. Das `service`-Präfix ist standardmäßig nicht im Typnamen enthalten.
4	Bereichsbezeichnung Die optionale Zeile besteht aus dem Token `scope`, dem ein Pluszeichen und eine durch Komma getrennte Liste von Bereichsnamen folgt. Bereichsnamen werden durch die `net.slp.useScopes`-Konfigurationseigenschaft definiert. Nur die für den Host konfigurierten Bereiche sollten in die Liste aufgenommen werden. Wenn keine Bereichszeile hinzugefügt wird, wird die Registrierung in allen Bereichen durchgeführt, für die `slpd` konfiguriert ist. Die Bereichszeile muss unmittelbar nach der URL-Zeile folgen. Anderenfalls werden Bereichsnamen als Attribute erkannt.
5 bis 8	Attributdefinitionen Nach der optionalen Bereichszeile besteht der größte Teil des Service-Advertisements aus Zeilen, die Attribut-/Wertlisten-Paare enthalten. Jedes Paar besteht aus dem Attribut-Tag, dem ein Gleichheitszeichen folgt, und einem Attributwert oder einer durch Komma getrennten Liste von Werten. Im vorangegangenen Beispiel für eine Proxyregistrierungsdatei enthält Zeile 8 eine Attributliste mit mehreren Werten. Alle anderen Listen haben einzelne Werte. Das Format für die Attributnamen und -Werte ist dasselbe wie bei netzerkgebundenen SLP-Meldungen.

Überlegungen zum Advertisement von veralteten Services

Im Allgemeinen ist das Modifizieren des Quellcodes zum Hinzufügen von SLP dem Schreiben eines SLP-fähigen Service vorzuziehen, der die SLP-API verwendet, um anstelle von anderen Services Advertisements durchzuführen. Das Modifizieren des Quellcodes ist auch der Verwendung der Proxyregistrierung vorzuziehen. Wenn Sie den Quellcode modifizieren, können Sie servicespezifische Funktionen hinzufügen und die Serviceverfügbarkeit genau verfolgen. Wenn der Quellcode nicht verfügbar ist, ist das Schreiben eines SLP-fähigen Hilfsservice, der Advertisements anstelle von anderen Services durchführt, der Verwendung der Proxyregistrierung vorzuziehen. Dieser Hilfsservice wird im Idealfall in die Service-Start-/Stopp-Prozedur integriert, die verwendet wird, um die Aktivierung und Deaktivierung zu steuern. Das Proxy-Advertisement ist normalerweise die dritte Option, wenn kein Quellcode zur Verfügung steht und das Schreiben eines eigenständigen SA nicht praktisch ist.

Proxy-Advertisements werden nur dann unterstützt, wenn `slpd` ausgeführt wird, damit die Proxyregistrierungsdatei gelesen werden kann. Es besteht keine direkte Verbindung zwischen dem Proxy-Advertisement und dem Service. Wenn ein Advertisement eine Zeitüberschreitung auslöst oder `slpd` angehalten wird, ist das Proxy-Advertisement nicht mehr verfügbar.

Wenn der Service deaktiviert wird, muss `slpd` gestoppt werden. Die serialisierte Registrierungsdatei wird bearbeitet, um das Proxy-Advertisement auszukommentieren oder zu entfernen, und `slpd` wird neu gestartet. Nach demselben Verfahren ist vorzugehen, wenn der Service neu gestartet oder neu installiert wird. Die fehlende Verbindung zwischen dem Proxy-Advertisement und dem Service ist ein großer Nachteil von Proxy-Advertisements.

◆ ◆ ◆ KAPITEL 11

11 SLP (Referenz)

In diesem Kapitel werden die SLP-Statuscodes und Meldungstypen beschrieben. Die SLP-Meldungstypen werden zusammen mit den entsprechenden Kürzeln und Funktionscodes aufgeführt. Die SLP-Statuscodes werden zusammen mit Beschreibungen und Funktionscodes aufgeführt, die verwendet werden, um anzuzeigen, dass eine Anforderung empfangen wurde (Code 0) oder dass der Empfänger beschäftigt ist.

Hinweis – Der SLP-Dämon (`slpd`) gibt nur Statuscodes für Unicast-Meldungen zurück.

SLP-Statuscodes

TABELLE 11–1 SLP-Statuscodes

Statustyp	Statuscode	Beschreibung
Kein Fehler	0	Die Anforderung wurde fehlerfrei bearbeitet.
LANGUAGE_NOT_SUPPORTED	1	Die AttrRqst- oder SrvRqst-Meldung zeigt an, dass im Bereich Daten für den Servicetyp enthalten sind, jedoch nicht in der angegebenen Sprache.
PARSE_ERROR	2	Die Meldung entspricht nicht der SLP-Syntax.
INVALID_REGISTRATION	3	Die SrvReg-Meldung ist problembehaftet (z. B. eine Null-Lebensdauer oder ein ausgelassener Sprachcode).
SCOPE_NOT_SUPPORTED	4	Die SLP-Meldung enthält keinen Bereich in ihrer Bereichsliste, die vom SA oder DA unterstützt wird, der auf die Anforderung geantwortet hat.
AUTHENTICATION_UNKNOWN	5	Der DA oder SA hat eine Anforderung erhalten, die sich auf eine nicht unterstützte SLP-SPI bezieht.

TABELLE 11–1 SLP-Statuscodes *(Fortsetzung)*

Statustyp	Statuscode	Beschreibung
AUTHENTICATION_ABSENT	6	Der UA oder DA hat nicht die erwartete URL und die entsprechende Attributauthentifizierung in der SrvReg-Meldung erhalten.
AUTHENTICATION_FAILED	7	Der UA oder DA erkennt einen Authentifizierungsfehler im Authentifizierungsblock.
VER_NOT_SUPPORTED	9	Die Meldung enthält eine nicht unterstützte Versionsnummer.
INTERNAL_ERROR	10	Im DA oder SA ist ein unbekannter Fehler aufgetreten (im Betriebssystem ist beispielsweise kein Dateispeicherplatz vorhanden).
DA_BUSY_NOW	11	Der UA oder SA muss erneut versuchen, den Vorgang mithilfe der exponentiellen Verzögerung auszuführen. Der DA ist mit der Verarbeitung anderer Meldungen beschäftigt.
OPTION_NOT_UNDERSTOOD	12	Der DA oder SA hat eine unbekannte Option aus dem obligatorischen Bereich erhalten.
INVALID_UPDATE	13	Der DA hat aufgrund eines nicht registrierten Service oder eines Service mit inkonsistenten Servicetypen eine SrvReg-Meldung ohne FRESH empfangen.
MSG_NOT_SUPPORTED	14	Der SA hat eine AttrRqst- oder SrvTypeRqst-Meldung erhalten, die nicht von ihm unterstützt wird.
REFRESH_REJECTED	15	Der SA hat eine SrvReg-Meldung oder eine teilweise SrvDereg-Meldung häufiger an einen DA gesendet, als dies im kleinsten Aktualisierungsintervall des DA definiert ist.

SLP-Meldungstypen

TABELLE 11–2 SLP-Meldungstypen

Meldungstyp	Kürzel	Funktionscode	Beschreibung
Serviceanforderung	`SrvRqst`	1	Eine von einem UA (zum Suchen von Services) oder von einem UA- oder SA-Server während der aktiven DA-Erkennung ausgegebene Meldung

TABELLE 11–2 SLP-Meldungstypen *(Fortsetzung)*

Meldungstyp	Kürzel	Funktionscode	Beschreibung
Serviceantwort	`SrvRply`	2	Die Antwort eines DA oder SA auf eine Serviceanforderung
Serviceregistrierung	`SrvReg`	3	Ermöglicht SAs, neue Advertisements zu registrieren, vorhandene Advertisements mit neuen und geänderten Attributen zu aktualisieren und URL-Lebensdauern zu aktualisieren
Entfernung der Serviceregistrierung	`SrvDereg`	4	Wird vom SA verwendet, um die Registrierung seiner Advertisements zu entfernen, wenn der bekannt gegebe Service nicht mehr verfügbar ist
Bestätigung	`SrvAck`	5	Die DA-Antwort auf eine Serviceanforderung eines DA oder eine Meldung bei Entfernung einer Serviceregistrierung
Attributanforderung	`AttrRqst`	6	Wird entweder über die URL oder den Servicetyp durchgeführt, um eine Liste von Attributen anzufordern
Attributantwort	`AttrRply`	7	Wird verwendet, um die Liste der Attribute zurückzugeben
DA-Advertisement	`DAAdvert`	8	Die DA-Antwort auf Multicast-Serviceanforderungen
Servicetypanforderung	`SrvTypeRqst`	9	Wird verwendet, um Informationen über registrierte Servicetypen einzuholen, die eine bestimmte Naming-Berechtigung haben und sich in bestimmten Bereichen befinden
Servicetypantwort	`SrvTypeRply`	10	Die Meldung, die als Antwort auf die Servicetypanforderung zurückgegeben wird
SA-Advertisement	`SAAdvert`	11	UAs verwenden `SAAdvert`, um SAs und deren Bereiche in Netzwerken zu erkennen, in denen keine DAs bereitgestellt sind.

TEIL IV

Mailservices – Themen

Dieser Abschnitt enthält eine Übersicht sowie aufgabenbezogene und Referenzinformationen zum Thema Mailservice.

◆ ◆ ◆ KAPITEL 12

Mailservices (Übersicht)

Mit der Einrichtung und Verwaltung eines elektronischen Mailservice sind komplexe Aufgaben verbunden, die wichtig für den täglichen Betrieb Ihres Netzwerks sind. Als Netzwerkadministrator müssen Sie möglicherweise einen vorhandenen Mailservice erweitern. Auch wäre es denkbar, dass Sie einen Mailservice in einem neuen Netzwerk oder in einem Teilnetz einrichten müssen. Die Kapitel, in denen Mailservices beschrieben werden, können Ihnen helfen, einen Mailservice für Ihr Netzwerk zu planen und einzurichten. Dieses Kapitel enthält Verweise auf Beschreibungen von neuen Funktionen in `sendmail` sowie eine Liste von anderen Informationsquellen. Außerdem enthält das Kapitel Übersichten der Software- und Hardwarekomponenten, die benötigt werden, um einen Mailservice einzurichten.

- „Neue Funktionen der Mailservices“ auf Seite 293
- „Weitere `sendmail`-Informationsquellen“ auf Seite 295
- „Einführung in die Komponenten von Mailservices“ auf Seite 295

Informationen zu den Verfahren, wie Mailservices eingerichtet und verwaltet werden, finden Sie in Kapitel 13, „Mailservices (Aufgaben)“. Weitere Informationen finden Sie unter „Übersicht der Schritte für Mailservices“ auf Seite 299.

Eine ausführliche Beschreibung der Komponenten von Mailservices finden Sie in Kapitel 14, „Mailservices (Referenz)“. Dieses Kapitel enthält zudem Beschreibungen der Mailservice-Programme und -Dateien, des Mail-Routing-Prozesses, der Interaktionen von `sendmail` mit Name Services und der Funktionen der Version 8.13 von `sendmail`. Lesen Sie dazu „Änderungen in Version 8.13 von `sendmail`“ auf Seite 392.

Neue Funktionen der Mailservices

Dieser Abschnitt enthält Informationen zu neuen Funktionen in verschiedenen Solaris-Versionen.

Änderungen in dieser Version

In Oracle Solaris 10 Update 10 wurden folgende Änderungen vorgenommen:

- Die Standardversion von sendmail wurde auf 8.14 aktualisiert.
- Die sendmail-Instanz wurde in zwei Instanzen geteilt, um für bessere Verwaltbarkeit des herkömmlichen Dämons (`svc:/network/smtp:sendmail`) und des Clientwarteschlangen-Betriebsprogramms (`svc:/network/smtp:sendmail-client`) zu sorgen.
- Das System kann so konfiguriert werden, dass die Konfigurationsdateien `sendmail.cf` und `submit.mc` automatisch neu erstellt werden. Informationen zu den erforderlichen Schritten finden Sie unter „So konfigurieren Sie die automatische Neuerstellung einer Konfigurationsdatei“ auf Seite 315.
- Der sendmail-Dämon wird standardmäßig im lokalen Dämonmodus ausgeführt. Der Modus "nur lokal" akzeptiert nur eingehende Mails vom lokalen Host oder Loopback-SMTP-Verbindungen. Beispielsweise würden Mails von einem cron-Job oder zwischen lokalen Benutzern akzeptiert werden. Abgehende Mails werden wie vorgesehen weitergeleitet, nur die eingehenden Mails werden geändert. Die Option `-bl` wird verwendet, um den Modus "nur lokal" auszuwählen, der auch als "Become Local"-Modus bekannt ist. Weitere Informationen zu diesem Modus finden Sie auf der Manpage `sendmail(1M)`. Anweisungen zur Rückkehr in den `-bd`- oder "Become Daemon"-Modus finden Sie unter „So verwenden Sie `sendmail` im offenen Modus“ auf Seite 316.

Änderungen in Solaris 10 1/06

Ab Solaris 10 1/06 unterstützt `sendmail` das SMTP mithilfe von TLS (Transport Layer Security). Weitere Informationen finden Sie hier:

- „Unterstützung für die Ausführung von SMTP mit TLS in Version 8.13 von `sendmail`“ auf Seite 392
- „So richten Sie SMTP zur Verwendung von TLS ein“ auf Seite 317

Eine vollständige Liste der Funktionen von Solaris 11 1/06 finden Sie unter *Neuerungen in Oracle Solaris 10 8/11*.

Änderungen in Solaris 10

`sendmail` 8.13 ist die Standardversion. Informationen zu Version 8.13 und anderen Änderungen finden Sie unter:

- „Zum Kompilieren von `sendmail` verwendete und nicht verwendete Flags“ auf Seite 352
- „`MILTER`, Mailfilter-API für `sendmail`“ auf Seite 354
- „Versionen der Konfigurationsdatei“ auf Seite 354

- „Verbesserung des Dienstprogramms `vacation`“ auf Seite 367
- „Inhalt des `/etc/mail/cf`-Verzeichnisses“ auf Seite 369
- „Änderungen in Version 8.13 von `sendmail`“ auf Seite 392
- „Unterstützung für TCP-Wrapper ab Version 8.12 von `sendmail`“ auf Seite 401

Zusätzlich wird der Mailservice von der Service Management Facility verwaltet. Administrative Maßnahmen an diesem Service, z. B. Aktivieren, Deaktivieren oder Neustarten, können mithilfe des Befehls `svcadm` vorgenommen werden. Der Status des Service kann mit dem Befehl `svcs` abgefragt werden. Weitere Informationen zur Service Management Facility finden Sie auf der Manpage `smf`(5) und in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*.

Weitere `sendmail`-Informationsquellen

Es folgt eine Liste von zusätzlichen Informationsquellen zu `sendmail` .

- Costales, Bryan. *sendmail, Third Edition*. O'Reilly & Associates, Inc., 2002.
- Homepage für `sendmail` – `http://www.sendmail.org`.
- Häufig gestellte Fragen (FAQs) zu `sendmail` – `http://www.sendmail.org/faq`.
- README-Datei für neue `sendmail`-Konfigurationsdateien – `http://www.sendmail.org/m4/readme.html`.
- Ein Leitfaden für Probleme im Zusammenhang mit der Umstellung auf neuere Versionen von `sendmail` – `http://www.sendmail.org/vendor/sun/`.

Einführung in die Komponenten von Mailservices

Viele Software- und Hardwarekomponenten werden benötigt, um einen Mailservice einzurichten. In den folgenden Abschnitten werden diese Komponenten kurz vorgestellt. Zudem enthalten diese Abschnitte Begriffe, die zur Beschreibung der Komponenten dienen.

Im ersten Abschnitt, „Übersicht der Softwarekomponenten“ auf Seite 295, werden die Begriffe definiert, die zur Erläuterung der Softwareelemente des Mail-Übermittelungssystems verwendet werden. Der nächste Abschnitt, „Übersicht der Hardwarekomponenten“ auf Seite 296, konzentriert sich auf die Funktionen der Hardwaresysteme in einer Mailkonfiguration.

Übersicht der Softwarekomponenten

In der folgenden Tabelle werden einige der Softwarekomponenten eines Mailsystems vorgestellt. Eine vollständige Beschreibung aller Softwarekomponenten finden Sie unter „Softwarekomponenten“ auf Seite 355.

Komponente	Beschreibung
`.forward`-Dateien	Dateien, die Sie im Home-Verzeichnis eines Benutzers einrichten können, um Mails umzuleiten oder automatisch an ein Programm zu senden
Mailbox	Eine Datei auf einem Mailserver, die das endgültige Ziel für E-Mail-Nachrichten ist
Mailadressen	Adressen, die den Namen des Empfängers und des Systems enthalten, an das eine Mail übermittelt wird
Mailaliase	Alternative Namen, die in Mailadressen verwendet werden
Mailwarteschlange	Eine Sammlung von Mails, die vom Mailserver verarbeitet werden müssen
postmaster	Ein spezieller Mailalias, der verwendet wird, um Probleme zu melden und Fragen zum Mailservice zu stellen
sendmail-Konfigurationsdatei	Eine Datei, die alle für das Mail-Routing erforderlichen Informationen enthält

Übersicht der Hardwarekomponenten

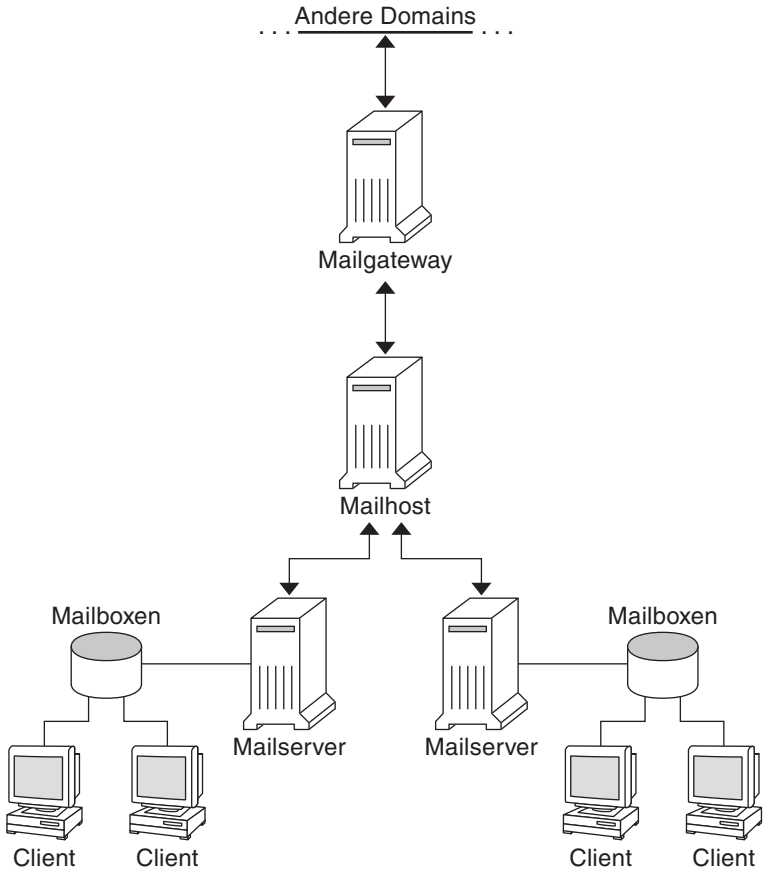
Für eine Mailkonfiguration sind drei Elemente erforderlich, die Sie im gleichen System kombinieren oder in separaten Systemen bereitstellen können.

- Ein Mailhost – ein System das so konfiguriert ist, dass es E-Mail-Adressen verarbeiten kann, die schwierig aufzulösen sind
- Mindestens ein Mailserver – ein System, das so konfiguriert ist, dass es eine oder mehrere Mailboxen enthalten kann
- Mailclients – Systeme, die auf Mails von einem Mailserver zugreifen

Wenn Benutzer mit Netzwerken außerhalb Ihrer Domäne kommunizieren sollen, müssen Sie ein viertes Element – ein Mailgateway – hinzufügen.

Abbildung 12–1 zeigt eine typische Konfiguration für die elektronische Übermittlung von Mails, die aus drei grundlegenden Mailelementen und einem Mailgateway besteht.

ABBILDUNG 12–1 Typische Konfiguration für die elektronische Übermittlung von Mails



Jedes Element wird ausführlich unter „Hardwarekomponenten“ auf Seite 363 beschrieben.

◆ ◆ ◆ KAPITEL 13

Mailservices (Aufgaben)

In diesem Kapitel wird beschrieben, wie Mailservices eingerichtet und verwaltet werden. Wenn Sie nicht mit der Verwaltung von Mailservices vertraut sind, lesen Sie die Einführung zu den Komponenten von Mailservices in Kapitel 12, „Mailservices (Übersicht)“. Dieses Kapitel enthält auch eine Beschreibung einer typischen Mailservice-Konfiguration (siehe Abbildung 12–1). Die folgende Liste hilft Ihnen bei der Suche nach Gruppen von verwandten Verfahren, die in diesem Kapitel beschrieben werden.

- „Übersicht der Schritte für Mailservices“ auf Seite 299
- „Einrichten von Mailservices (Übersicht der Schritte)“ auf Seite 304
- „Ändern der sendmail-Konfiguration (Übersicht der Schritte)“ auf Seite 313
- „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323
- „Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)“ auf Seite 336
- „Verwalten von `.forward`-Dateien (Übersicht der Schritte)“ auf Seite 339
- „Fehlerbehebungsverfahren und Tipps für Mailservices (Übersicht der Schritte)“ auf Seite 342

Eine ausführliche Beschreibung der Komponenten von Mailservices finden Sie in Kapitel 14, „Mailservices (Referenz)“. Dieses Kapitel enthält zudem Beschreibungen der Mailservice-Programme und Dateien, des Mail-Routing-Prozesses, der Interaktionen von `sendmail` mit Name Services und der Funktionen der Version 8.13 von `sendmail`, die nicht vollständig auf der Manpage `sendmail(1M)` beschrieben sind.

Übersicht der Schritte für Mailservices

Die folgende Tabelle verweist auf weitere Aufgaben, die für eine bestimmte Gruppe von Verfahren vorgesehen sind.

Aufgabe	Beschreibung	Siehe
Einrichten von Mailservices	Verwenden Sie diese Verfahren, um die einzelnen Komponenten Ihres Mailservices einzurichten. Erfahren Sie, wie ein Mailserver, ein Mailclient, ein Mailhost und ein Mailgateway eingerichtet werden. Erfahren Sie, wie DNS mit `sendmail` verwendet wird.	„Einrichten von Mailservices (Übersicht der Schritte)“ auf Seite 304
Ändern der sendmail-Konfiguration	Verwenden Sie diese Verfahren, um Konfigurationsdateien oder Serviceeigenschaften zu ändern.	„Ändern der sendmail-Konfiguration (Übersicht der Schritte)“ auf Seite 313
Verwalten von Mailaliasdateien	Verwenden Sie diese Verfahren, um Aliasing für Ihr Netzwerk bereitzustellen. Erfahren Sie, wie Sie Einträge in NIS+-Tabellen verwalten. Erfahren Sie außerdem, wie eine NIS-Tabelle, ein lokaler Mailalias, eine verschlüsselte Zuordnungsdatei und ein Postmaster-Alias eingerichtet werden.	„Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323
Verwalten der Mailwarteschlange	Verwenden Sie diese Verfahren, um eine reibungslose Verarbeitung der Warteschlange zu gewährleisten. Erfahren Sie, wie die Mailwarteschlange angezeigt und verschoben, die Verarbeitung der Mailwarteschlange erzwungen und ein Teil der Mailwarteschlange ausgeführt wird. Erfahren Sie außerdem, wie die alte Mailwarteschlange ausgeführt wird.	„Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)“ auf Seite 336
Verwalten von `.forward`-Dateien	Verwenden Sie diese Verfahren, um `.forward`-Dateien zu deaktivieren oder den Suchpfad der `.forward`-Datei zu ändern. Erfahren Sie zudem, wie Sie Benutzern gestatten, die `.forward`-Datei zu verwenden, indem Sie `/etc/shells` erstellen und auffüllen.	„Verwalten von `.forward`-Dateien (Übersicht der Schritte)“ auf Seite 339
Fehlerbehebungsverfahren und Tipps für Mailservices	Verwenden Sie diese Verfahren und Tipps, um Probleme mit Ihrem Mailservices zu beheben. Erfahren Sie, wie die Mailkonfiguration, Mailaliase, `sendmail`-Regellisten, Verbindungen mit anderen Systemen und Protokollmeldungen geprüft und verifiziert werden. Erfahren Sie zudem, wo weitere Informationen zur Maildiagnose zu finden sind.	„Fehlerbehebungsverfahren und Tipps für Mailservices (Übersicht der Schritte)“ auf Seite 342

Aufgabe	Beschreibung	Siehe
Auflösen von Fehlermeldungen	Verwenden Sie die in diesem Abschnitt enthaltenen Informationen, um Mailfehlermeldungen aufzulösen.	„Auflösen von Fehlermeldungen“ auf Seite 348

Planen Ihres Mailsystems

Im Folgenden wird beschrieben, was Sie in Ihrem Planungsprozess berücksichtigen sollten.

- Stellen Sie fest, welche Mailkonfiguration am besten Ihren Erfordernissen entspricht. In diesem Abschnitt werden zwei grundlegende Mailkonfigurationstypen beschrieben, und es wird kurz aufgelistet, was Sie benötigen, um jede Konfiguration einzurichten. Wenn Sie ein neues Mailsystem einrichten oder ein vorhandenes Mailsystem erweitern müssen, werden Sie in diesem Abschnitt u. U. nützliche Informationen finden. „Nur lokale Mail“ auf Seite 301: Hier wird der erste Konfigurationstyp beschrieben. Unter „Lokale Mails und eine Remote-Verbindung“ auf Seite 302 wird der zweite Typ beschrieben.
- Wählen Sie nach Bedarf die Systeme aus, die als Mailserver, Mailhosts und Mailgateways fungieren sollen.
- Erstellen Sie eine Liste von allen Mailclients, für die Sie ein Service bereitstellen, und geben Sie auch die Adresse der Mailboxen dieser Clients an. Diese Liste kann Ihnen helfen, wenn Sie vorhaben, Mailaliase für Ihre Benutzer zu erstellen.
- Legen Sie fest, wie Aliase aktualisiert und Mails weitergeleitet werden. Sie können eine `Alias`-Mailbox für Benutzer einrichten, an die Anfragen zur Weiterleitung von Mails gesendet werden können. Benutzer können diese Mailbox auch dazu verwenden, um Anfragen zu senden, die Änderungen an ihren standardmäßigen Mailaliasen betreffen. Wenn Ihr System NIS oder NIS+ verwendet, können Sie die Weiterleitung von Mails verwalten und müssen dies nicht von den Benutzern verlangen. Unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 wird eine Liste von Aufgaben bereitgestellt, die sich auf das Aliasing beziehen. „Verwalten von `.forward`-Dateien (Übersicht der Schritte)“ auf Seite 339 stellt eine Liste von Aufgaben bereit, die sich auf die Verwaltung von `.forward` -Dateien beziehen.

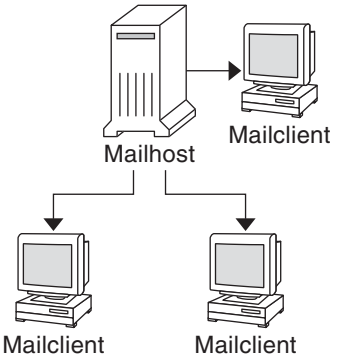
Nachdem Sie den Planungsprozess abgeschlossen haben, richten Sie die Systeme an Ihrem Standort ein, sodass diese die Funktionen erfüllen, die unter „Einrichten von Mailservices (Übersicht der Schritte)“ auf Seite 304 beschrieben sind. Weitere aufgabenbezogene Informationen finden Sie unter „Übersicht der Schritte für Mailservices“ auf Seite 299.

Nur lokale Mail

Die einfachste Mailkonfiguration (siehe Abbildung 13–1) besteht aus zwei oder mehreren Workstations, die mit einem Mailhost verbunden sind. Es handelt sich ausschließlich um lokale

Mails. Mails werden auf allen Clients auf den lokalen Festplatten gespeichert, und die Clients fungieren als Mailserver. Mailadressen werden mithilfe von `/etc/mail/aliases`-Dateien analysiert.

ABBILDUNG 13–1 Lokale Mailkonfiguration



Um diesen Mailkonfigurationstyp einzurichten, benötigen Sie Folgendes:

- Die standardmäßige `/etc/mail/sendmail.cf`-Datei auf jedem Mailclientsystem, die nicht bearbeitet werden muss.
- Ein Server, der als Mailhost angegeben ist. Wenn Sie NIS oder NIS+ ausführen, können Sie diese Angabe machen, indem Sie `mailhost.`*domain-name* der `/etc/hosts`-Datei auf dem Mailhost hinzufügen. Wenn Sie einen anderen Name Service wie beispielsweise DNS oder LDAP ausführen, müssen Sie zusätzliche Informationen in der `/etc/hosts`-Datei angeben. Siehe „So richten Sie einen Mailhost ein“ auf Seite 309.
- Wenn Sie einen anderen Name Service als NIS oder NIS+ verwenden, müssen Sie die `/etc/mail/aliases`-Dateien auf einem System abgleichen, das eine lokale Mailbox besitzt.
- Genügend Platz in `/var/mail` auf jedem Mailclientsystem zur Aufnahme der Mailboxen.

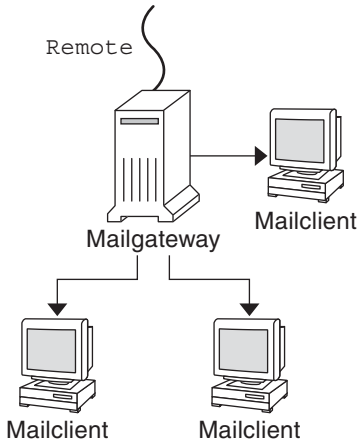
Weitere aufgabenbezogene Informationen für die Einrichtung Ihres Mailservice finden Sie unter „Einrichten von Mailservices“ auf Seite 304. Wenn Sie ein bestimmtes Verfahren zur Einrichtung Ihres Mailservice benötigen, finden Sie die erforderlichen Informationen unter „Einrichten von Mailservices (Übersicht der Schritte)“ auf Seite 304.

Lokale Mails und eine Remote-Verbindung

Die am häufigsten verwendete Mailkonfiguration in einem kleinen Netzwerk ist in Abbildung 13–2 dargestellt. Ein System besteht aus einem Mailserver, dem Mailhost und dem

Mailgateway, das die Remote-Verbindung bereitstellt. Mails werden mithilfe der `/etc/mail/aliases`-Dateien auf dem Mailgateway verteilt. Es ist kein Name Service erforderlich.

ABBILDUNG 13–2 Lokale Mailkonfiguration mit einer UUCP-Verbindung



In dieser Konfiguration setzen Sie voraus, dass die Mailclients ihre Maildateien von `/var/mail` auf dem Mailhost einhängen. Um diesen Mailkonfigurationstyp einzurichten, benötigen Sie Folgendes:

- Die standardmäßige `/etc/mail/sendmail.cf`-Datei auf jedem Mailclientsystem. Diese Datei muss nicht bearbeitet werden.
- Ein Server, der als Mailhost angegeben ist. Wenn Sie NIS oder NIS+ ausführen, können Sie diese Angabe machen, indem Sie `mailhost.`*domain-name* der `/etc/hosts`-Datei auf dem Mailhost hinzufügen. Wenn Sie einen anderen Name Service wie beispielsweise DNS oder LDAP ausführen, müssen Sie zusätzliche Informationen in der `/etc/hosts`-Datei angeben. Siehe „So richten Sie einen Mailhost ein“ auf Seite 309.
- Wenn Sie einen anderen Name Service als NIS oder NIS+ verwenden, müssen Sie die `/etc/mail/aliases`-Dateien auf einem System abgleichen, das eine lokale Mailbox besitzt.
- Genügend Platz in `/var/mail` auf dem Mailserver zur Aufnahme der Client-Mailboxen.

Aufgabenbezogene Informationen zur Einrichtung Ihres Mailservices finden Sie unter „Einrichten von Mailservices“ auf Seite 304. Wenn Sie ein bestimmtes Verfahren zur Einrichtung Ihres Mailservice benötigen, finden Sie die erforderlichen Informationen unter „Einrichten von Mailservices (Übersicht der Schritte)“ auf Seite 304.

Einrichten von Mailservices (Übersicht der Schritte)

In der folgenden Tabelle werden die Verfahren zum Einrichten von Mailservices beschrieben.

Aufgabe	Beschreibung	Siehe
Einrichten eines Mailservers	Schritte, die auszuführen sind, damit ein Server Mails weiterleiten kann	„Einrichten eines Mailservers“ auf Seite 305
Einrichten eines Mailclients	Schritte, die auszuführen sind, damit ein Benutzer Mails empfangen kann	„So richten Sie einen Mailclient ein“ auf Seite 307
Einrichten eines Mailhosts	Schritte zum Einrichten eines Mailhosts, der E-Mail-Adressen auflösen kann	„So richten Sie einen Mailhost ein“ auf Seite 309
Einrichten eines Mailgateways	Schritte zum Verwalten der Kommunikation mit Netzwerken außerhalb Ihrer Domain	„So richten Sie ein Mailgateway ein“ auf Seite 310
Verwenden von DNS mit `sendmail`	Schritte zur Aktivierung von DNS-Suchvorgängen	„So verwenden Sie DNS mit `sendmail`“ auf Seite 312

Einrichten von Mailservices

Sie können rasch ein Mailservice einrichten, wenn Ihre Site keine Verbindungen mit E-Mail-Services außerhalb Ihres Unternehmens bereitstellt oder wenn Ihr Unternehmen sich in einer einzelnen Domain befindet.

Zur Übermittlung von Mails sind zwei Konfigurationstypen für lokale Mails erforderlich. Eine Darstellung dieser Konfigurationen wird in Abbildung 13–1 unter „Nur lokale Mail“ auf Seite 301 gezeigt. Zur Übermittlung von Mails sind zwei weitere Konfigurationen für die Kommunikation mit Netzwerken außerhalb Ihrer Domain erforderlich. Eine Darstellung dieser Konfigurationen wird in Abbildung 12–1 unter „Übersicht der Hardwarekomponenten“ auf Seite 296 oder in Abbildung 13–2 unter „Lokale Mails und eine Remote-Verbindung“ auf Seite 302 gezeigt. Sie können diese Konfigurationen auf demselben System kombinieren oder auf separaten Systemen bereitstellen. Wenn sich beispielsweise Ihre Mailhost- und Mailserver-Funktionen auf demselben System befinden, folgen Sie den Hinweisen in diesem Abschnitt, um das betreffenden System als Mailhost einzurichten. Anschließend folgen Sie den Hinweisen in diesem Abschnitt, um dasselbe System als Mailserver einzurichten.

Hinweis – Die folgenden Verfahren zum Einrichten eines Mailservers und eines Mailclients gelten, wenn Mailboxen über NFS eingehängt werden. Mailboxen werden jedoch normalerweise in lokal eingehängten `/var/mail`-Verzeichnissen verwaltet, wodurch die folgenden Verfahren nicht nötig sind.

Einrichten eines Mailservers

Zum Einrichten eines Mailservers, der nur die Mails von lokalen Benutzern weiterleitet, sind keine bestimmten Schritte erforderlich. Für den Benutzer muss ein Eintrag in der Passwortdatei oder im Namespace vorhanden sein. Außerdem benötigt der Benutzer für Mails, die bereitgestellt werden sollen, ein lokales Home-Verzeichnis, damit die `~/.forward`-Datei überprüft werden kann. Aus diesem Grunde werden Home-Verzeichnisserver oft als Mailserver eingerichtet. Weitere Informationen zum Mailserver finden Sie unter „Hardwarekomponenten“ auf Seite 363 in Kapitel 14, „Mailservices (Referenz)“.

Der Mailserver kann die Mails vieler Mailclients weiterleiten. Dieser Mailservertyp muss einen angemessenen Spoolbereich für Clientmailboxen haben.

Hinweis – Das `mail.local`-Programm erstellt automatisch Mailboxen im `/var/mail`-Verzeichnis, wenn eine Mail zum ersten Mal übermittelt wird. Sie müssen keine speziellen Mailboxen für Ihre Mailclients erstellen.

Damit Clients Zugriff auf ihre Mailboxen haben, muss das `/var/mail` -Verzeichnis für das Remote-Einhängen verfügbar sein. Als Alternative dazu sollte ein Service wie POP (Post Office Protocol) oder IMAP (Internet Message Access Protocol) vom Server aus verfügbar sein. In der folgenden Aufgabe wird gezeigt, wie Sie einen Mailserver mithilfe des `/var/mail`-Verzeichnisses einrichten. Auf die Bereitstellung von Konfigurationsrichtlinien für POP oder IMAP wird im vorliegenden Dokument nicht eingegangen.

Stellen Sie für die folgende Aufgabe sicher, dass die `/etc/dfs/dfstab`-Datei anzeigt, dass das `/var/mail`-Verzeichnis exportiert wird.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stoppen Sie `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Prüfen Sie, ob das `/var/mail` -Verzeichnis für den Remote-Zugriff verfügbar ist.

```
# share
```

Wenn das `/var/mail`-Verzeichnis aufgeführt wird, fahren Sie mit Schritt 5 fort.

Wenn das `/var/mail`-Verzeichnis nicht aufgeführt wird oder wenn keine Liste angezeigt wird, fahren Sie mit dem entsprechenden Teilschritt fort.

a. (Optional) Wenn keine Liste angezeigt wird, starten Sie die NFS-Services.

Wenden Sie das unter „So richten Sie die automatische Freigabe von Dateisystemen ein“ auf Seite 87 beschriebene Verfahren an, um mithilfe des `/var/mail`-Verzeichnisses die NFS-Services zu starten.

b. (Optional) Wenn das `/var/mail` -Verzeichnis nicht in der Liste enthalten ist, fügen Sie das Verzeichnis in `/etc/dfs/dfstab` ein.

Fügen Sie die folgende Befehlszeile in die Datei `/etc/dfs/dfstab` ein.

```
share -F nfs -o rw /var/mail
```

4 Machen Sie das Dateisystem für das Einhängen verfügbar.

```
# shareall
```

5 Stellen Sie sicher, dass Ihr Name Service gestartet wurde.

a. (Optional) Wenn Sie NIS ausführen, verwenden Sie den folgenden Befehl:

```
# ypwhich
```

Weitere Informationen finden Sie auf der Manpage `ypwhich(1)`).

b. (Optional) Wenn Sie NIS+ ausführen, verwenden Sie den folgenden Befehl:

```
# nisls
```

Weitere Informationen finden Sie auf der Manpage `nisls(1)`.

c. (Optional) Wenn Sie DNS ausführen, verwenden Sie den folgenden Befehl:

```
# nslookup hostname
```

hostname Verwenden Sie Ihren Hostnamen.

Weitere Informationen finden Sie auf der Manpage `nslookup(1M)`.

d. (Optional) Wenn Sie LDAP ausführen, verwenden Sie den folgenden Befehl:

```
# ldaplist
```

Weitere Informationen finden Sie auf der Manpage `ldaplist(1)`.

6 Starten Sie `sendmail` neu.

```
# svcadm enable network/smtp:sendmail
```

▼ So richten Sie einen Mailclient ein

Bei einem Mailclient handelt es sich um einen Benutzer von Mailservices mit einer Mailbox auf einem Mailserver. Außerdem ist bei einem Mailclient ein Mailalias in der `/etc/mail/aliases`-Datei enthalten, die auf die Adresse der Mailbox verweist.

Hinweis – Sie können einen Mailclient auch einrichten, indem Sie einen Service (z. B. POP (Post Office Protocol) oder IMAP (Internet Message Access Protocol)) verwenden. Auf die Bereitstellung von Konfigurationsrichtlinien für POP oder IMAP wird jedoch im vorliegenden Dokument nicht eingegangen.

---

1 Melden Sie sich als Superuser beim System des Mailclients oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stoppen Sie `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Stellen Sie sicher, dass `/var/mail`-Einhängepunkt auf dem System des Mailclients vorhanden ist.

Der Einhängepunkt muss während des Installationsvorgangs erstellt worden sein. Sie können `ls` verwenden, um sicherzustellen, dass das Dateisystem vorhanden ist. Im folgenden Beispiel wird die Antwort gezeigt, die Sie erhalten, wenn das Dateisystem nicht erstellt wurde.

```
# ls -l /var/mail
/var/mail not found
```

4 Stellen Sie sicher, dass keine Dateien im `/var/mail` -Verzeichnis enthalten sind.

Wenn Maildateien in diesem Verzeichnis enthalten sind, entfernen Sie sie, sodass sie nicht berücksichtigt werden, wenn das `/var/mail`-Verzeichnis vom Server eingehängt wird.

5 Hängen Sie das `/var/mail`-Verzeichnis vom Mailserver ein.

Sie können das Mailverzeichnis automatisch oder beim Booten einhängen.

a. (Optional) Hängen Sie `/var/mail` automatisch ein.

Fügen Sie einen Eintrag wie den folgenden in die `/etc/auto_direct` -Datei ein:

```
/var/mail -rw,hard,actimeo=0 server:/var/mail
```

server Verwenden Sie den zugewiesenen Servernamen.

b. (Optional) Hängen Sie `/var/mail` während des Bootens ein.

Fügen Sie den folgenden Eintrag in die `/etc/vfstab` -Datei ein. Dieser Eintrag gestattet die Verwendung des `/var/mail`-Verzeichnisses auf dem Mailserver, der zum Einhängen des lokalen `/var/mail`-Verzeichnisses angegeben wurde.

server`:/var/mail - /var/mail nfs - no rw,hard,actimeo=0`

Die Mailbox des Clients wird automatisch eingehängt, wenn das System neu gebootet wird. Wenn Sie das System nicht neu booten, geben Sie zum Booten der Client-Mailbox den folgenden Befehl ein:

```
# mountall
```

Achtung – Damit die Sperrung und der Zugriff auf Mailboxen ordnungsgemäß funktionieren, müssen Sie die Option `actimeo=0` angeben, wenn Sie Mails von einem NFS-Server einhängen.

6 Aktualisieren Sie `/etc/hosts`.

Bearbeiten Sie die `/etc/hosts`-Datei und fügen Sie einen Eintrag für den Mailserver hinzu. Dieser Schritt ist nicht erforderlich, wenn Sie einen Name Service verwenden.

```
# cat /etc/hosts
#
# Internet host table
#
..
IP-address      mailhost  mailhost  mailhost.example.com
```

IP-address Verwenden Sie die zugewiesenen IP-Adressen.

example.com Verwenden Sie die zugewiesene Domain.

mailhost Verwenden Sie den zugewiesenen Mailhost.

Weitere Informationen finden Sie auf der Manpage `hosts(4)`.

7 Fügen Sie einen Eintrag für den Client in eine der Aliasdateien ein.

Eine Übersicht der Schritte zum Verwalten von Mailaliasdateien finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323. Beachten Sie, dass das `mail.local`-Programm automatisch Mailboxen im `/var/mail`-Verzeichnis erstellt, wenn eine Mail zum ersten Mal übermittelt wird. Sie müssen keine speziellen Mailboxen für Ihre Mailclients erstellen.

8 Starten Sie `sendmail` neu.

```
# svcadm enable network/smtp:sendmail
```

▼ So richten Sie einen Mailhost ein

Ein Mailhost löst E-Mail-Adressen auf und leitet Mails innerhalb Ihrer Domain weiter. Zur Verwendung als Mailhost eignet sich ein System, das eine Remote-Verbindung für Ihr System bereitstellt oder Ihr Netzwerk mit einer übergeordneten Domain verbindet. Anhand des folgenden Verfahrens wird aufgezeigt, wie ein Mailhost eingerichtet wird.

1 Melden Sie sich als Superuser beim Mailhostsystem oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stoppen Sie `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Prüfen Sie die Konfiguration des Hostnamens.

Führen Sie das `check-hostname`-Skript aus, um sicherzustellen, dass `sendmail` den voll qualifizierten Hostnamen für diesen Server identifizieren kann.

```
% /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

Wenn dieses Skript nicht den voll qualifizierten Hostnamen identifizieren kann, müssen Sie den voll qualifizierten Hostnamen als ersten Alias für den Host in `/etc/hosts` hinzufügen.

4 Aktualisieren Sie die `/etc/hosts`-Datei.

Wählen Sie den entsprechenden Schritt, um fortzufahren.

a. (Optional) Wenn Sie NIS oder NIS+ verwenden, bearbeiten Sie die `/etc/hosts`-Datei auf dem System, das als neuer Mailhost verwendet wird.

Fügen Sie hinter der IP-Adresse und dem Systemnamen des Mailhostsystems die Worte `mailhost` und `mailhost.`*domain* ein.

IP-address mailhost `mailhost mailhost.`*domain* `loghost`

IP-address Verwenden Sie die zugewiesene IP-Adresse.

mailhost Verwenden Sie den Systemnamen des Mailhostsystems.

domain Verwenden Sie den erweiterten Domainnamen.

Das System ist jetzt als Mailhost benannt. Die *Domain* muss identisch mit der Zeichenfolge sein, die als Name der Subdomain in der Ausgabe des folgenden Befehls angegeben ist.

```
% /usr/lib/sendmail -bt -d0 </dev/null
Version 8.13.1+Sun
 Compiled with: LDAPMAP MAP_REGEX LOG MATCHGECOS MIME7TO8 MIME8TO7
```

```
                NAMED_BIND NDBM NETINET NETINET6 NETUNIX NEWDB NIS
                NISPLUS QUEUE SCANF SMTP USERDB XDEBUG

============ SYSTEM IDENTITY (after readcf) ============
      (short domain name) $w = phoenix
  (canonical domain name) $j = phoenix.example.com
         (subdomain name) $m = example.com
               (node name) $k = phoenix
========================================================
```

Das folgende Beispiel zeigt, wie die `hosts`-Datei aussehen muss, nachdem diese Änderungen vorgenommen wurden.

```
# cat /etc/hosts
#
# Internet host table
#
172.31.255.255   localhost
192.168.255.255  phoenix mailhost mailhost.example.com loghost
```

b. (Optional) Wenn Sie NIS oder NIS+ nicht verwenden, bearbeiten Sie die `/etc/hosts`-Datei auf jedem System im Netzwerk.

Erstellen Sie den folgenden Eintrag.

IP-address mailhost `mailhost` *mailhost.domain* `loghost`

5 Starten Sie `sendmail` neu.

```
# svcadm enable network/smtp:sendmail
```

6 Prüfen Sie Ihre Mailkonfiguration.

Anweisungen finden Sie unter „So prüfen Sie die Mailkonfiguration“ auf Seite 343.

Hinweis – Weitere Informationen zu Mailhosts finden Sie unter „Hardwarekomponenten“ auf Seite 363 in Kapitel 14, „Mailservices (Referenz)“.

▼ So richten Sie ein Mailgateway ein

Ein Mailgateway dient zur Verwaltung der Kommunikation mit Netzwerken außerhalb Ihrer Domain. Der Mailer des sendenden Mailgateways kann sich an den Mailer des empfangenden Systems anpassen.

Zur Verwendung als Mailgateway eignet sich ein System, das mit dem Ethernet und Telefonleitungen verbunden ist. Es eignet sich auch ein System, das als Router für das Internet konfiguriert ist. Sie können den Mailhost oder ein anderes System als Mailgateway konfigurieren. Sie haben die Möglichkeit, mehrere Mailgateways für Ihre Domain zu konfigurieren. Wenn Sie UUCP-Verbindungen (UNIX-to-UNIX Copy Program) verwenden, konfigurieren Sie das System (oder die Systeme) mit UUCP-Verbindungen als Mailgateway.

1. **Melden Sie sich als Superuser beim Mailgateway oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `sendmail`.**

   ```
   # svcadm disable -t network/smtp:sendmail
   ```

3. **Prüfen Sie die Konfiguration des Hostnamens.**

   Führen Sie das `check-hostname`-Skript aus, um sicherzustellen, dass `sendmail` den voll qualifizierten Hostnamen für diesen Server identifizieren kann.

   ```
   # /usr/sbin/check-hostname
   hostname phoenix OK: fully qualified as phoenix.example.com
   ```

   Wenn dieses Skript nicht den voll qualifizierten Hostnamen identifizieren kann, müssen Sie den voll qualifizierten Hostnamen als ersten Alias für den Host in `/etc/hosts` hinzufügen. Hilfe bei diesem Schritt erhalten Sie unter Schritt 4 des Abschnitts „So richten Sie einen Mailhost ein“ auf Seite 309.

4. **Stellen Sie sicher, dass Ihr Name Service gestartet wurde.**

   a. **(Optional) Wenn Sie NIS ausführen, verwenden Sie den folgenden Befehl:**

      ```
      # ypwhich
      ```

      Weitere Informationen finden Sie auf der Manpage `ypwhich(1)`).

   b. **(Optional) Wenn Sie NIS+ ausführen, verwenden Sie den folgenden Befehl:**

      ```
      # nisls
      ```

      Weitere Informationen finden Sie auf der Manpage `nisls(1)`.

   c. **(Optional) Wenn Sie DNS ausführen, verwenden Sie den folgenden Befehl:**

      `# nslookup` *hostname*

      hostname Verwenden Sie Ihren Hostnamen.

      Weitere Informationen finden Sie auf der Manpage `nslookup(1M)`.

   d. **(Optional) Wenn Sie LDAP ausführen, verwenden Sie den folgenden Befehl:**

      ```
      # ldaplist
      ```

      Weitere Informationen finden Sie auf der Manpage `ldaplist(1)`.

5. **Starten Sie `sendmail` neu.**

   ```
   # svcadm enable network/smtp:sendmail
   ```

6 **Prüfen Sie Ihre Mailkonfiguration.**

Anweisungen finden Sie unter „So prüfen Sie die Mailkonfiguration“ auf Seite 343.

Hinweis – Weitere Informationen zum Mailgateway finden Sie unter „Hardwarekomponenten“ auf Seite 363 in Kapitel 14, „Mailservices (Referenz)“.

▼ So verwenden Sie DNS mit `sendmail`

Der Name Service DNS unterstützt keine Aliase für Einzelpersonen. Dieser Name Service unterstützt Aliase für Hosts oder Domains, die MX-Datensätze (Mail Exchanger) und `CNAME`-Datensätze verwenden. Sie können Hostnamen, Domainnamen oder beides in der DNS-Datenbank angeben. Weitere Informationen zu `sendmail` und DNS finden Sie unter „Interaktionen von `sendmail` mit Name Services“ auf Seite 386 in Kapitel 14, „Mailservices (Referenz)“ oder im *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Aktivieren Sie DNS-Host-Suchvorgänge (nur NIS+).**

Bearbeiten Sie die `/etc/nsswitch.conf`-Datei und entfernen Sie das Zeichen `#` aus der `hosts`-Definition, die das `dns`-Flag enthält. Der Hosteintrag muss das `dns`-Flag enthalten (siehe folgendes Beispiel), damit die DNS-Host-Aliase verwendet werden können.

```
# grep hosts /etc/nsswitch.conf
#hosts:     nisplus [NOTFOUND=return] files
hosts:      dns nisplus [NOTFOUND=return] files
```

3 **Prüfen Sie, ob ein Eintrag für `mailhost` und ein `mailhost.`*domain* vorhanden ist.**

Verwenden Sie `nslookup`, um sicherzustellen, dass ein Eintrag für `mailhost` und `mailhost.`*domain* in der DNS-Datenbank vorhanden ist. Weitere Informationen finden Sie auf der Manpage `nslookup(1M)`.

Ändern der sendmail-Konfiguration (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Erstellen einer `sendmail`-Konfigurationsdatei	Wenden Sie dieses Verfahren an, um Ihre `sendmail.cf`-Datei zu bearbeiten. Es ist ein Beispiel für das Maskieren von Domains enthalten.	„So erstellen Sie eine neue `sendmail.cf`-Datei“ auf Seite 314
Einrichten eines virtuellen Hosts	Schritte zum Konfigurieren von sendmail, damit Mails für mehr als eine Domain akzeptiert werden	„Einrichten eines virtuellen Hosts“ auf Seite 315
Einrichten der automatischen Neuerstellung der sendmail-Konfigurationsdatei	Wenden Sie dieses Verfahren an, um den sendmail-Service zu modifizieren, sodass die Konfigurationsdateien `sendmail.cf` und `submit.mc` nach einem Upgrade automatisch neu erstellt werden.	„So konfigurieren Sie die automatische Neuerstellung einer Konfigurationsdatei“ auf Seite 315
Ausführen von `sendmail` im offenen Modus	Wenden Sie dieses Verfahren zum Modifizieren der Eigenschaften des sendmail-Service an, um den offenen Modus zu aktivieren.	„So verwenden Sie `sendmail` im offenen Modus“ auf Seite 316
Einrichten von SMTP zur Verwendung der TLS (Transport Layer Security, Transportschichtsicherheit)	Wenden Sie dieses Verfahren zum Aktivieren von SMTP an, um sichere Verbindungen mit TLS zu gewährleisten.	„So richten Sie SMTP zur Verwendung von TLS ein“ auf Seite 317
Verwalten der Mailübermittlung mithilfe einer alternativen Konfiguration	Wenden Sie dieses Verfahren an, um Mailübermittlungsprobleme zu vermeiden, die auftreten können, wenn der Master-Dämon deaktiviert ist.	„So verwalten Sie die Mailübermittlung mithilfe einer alternativen Konfiguration von `sendmail.cf`“ auf Seite 322

Ändern der sendmail-Konfiguration

Informationen zum Erstellen der Konfigurationsdatei finden Sie unter „So erstellen Sie eine neue `sendmail.cf`-Datei“ auf Seite 314. Obwohl Sie weiterhin ältere Versionen von `sendmail.cf`-Dateien verwenden können, empfiehlt es sich, das neue Format zu verwenden.

Weitere Informationen finden Sie im Folgenden.

- `/etc/mail/cf/README` enthält eine vollständige Beschreibung des Konfigurationsverfahrens.
- `http://www.sendmail.org` stellt Online-Infrastruktur zur `sendmail`-Konfiguration bereit.
- Einige weitere Informationen finden Sie unter „Versionen der Konfigurationsdatei“ auf Seite 354 und „`sendmail`-Konfigurationsdatei“ auf Seite 378 in Kapitel 14, „Mailservices (Referenz)“.

- Informationen unter „Zusätzliche und überarbeitete m4-Konfigurationsmakros ab Version 8.12 von sendmail“ auf Seite 408 sind ebenfalls zu empfehlen.

▼ So erstellen Sie eine neue sendmail.cf-Datei

Das folgende Verfahren zeigt, wie eine neue Konfigurationsdatei erstellt wird.

Hinweis – /usr/lib/mail/cf/main-v7sun.mc ist jetzt /etc/mail/cf/cf/sendmail.mc.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Stoppen Sie sendmail.

```
# svcadm disable -t network/smtp:sendmail
```

3 Erstellen Sie eine Kopie der Konfigurationsdateien, die Sie ändern.

```
# cd /etc/mail/cf/cf
# cp sendmail.mc myhost.mc
```

myhost Legen Sie einen neuen Namen für Ihre .mc-Datei fest.

4 Bearbeiten Sie die neuen Konfigurationsdateien (beispielsweise *myhost*.mc), falls nötig).

Fügen Sie beispielsweise die folgende Befehlszeile hinzu, um die Domainmaskierung zu ermöglichen.

```
# cat myhost.mc
..
MASQUERADE_AS(‘host.domain’)
```

host.domain Verwenden Sie den gewünschten Hostnamen und den gewünschten Domainnamen.

In diesem Beispiel bewirkt MASQUERADE_AS, dass gesendete Mails gekennzeichnet werden, wodurch darauf hingewiesen wird, dass diese Mails ursprünglich von *host.domain* kommen (und nicht von $j).

5 Erstellen Sie die Konfigurationsdatei mithilfe von m4.

```
# /usr/ccs/bin/make myhost.cf
```

6 Prüfen Sie die neue Konfigurationsdatei, indem Sie die neue Datei mithilfe der Option -C angeben.

```
# /usr/lib/sendmail -C myhost.cf -v testaddr </dev/null
```

Während mithilfe dieses Befehls Nachrichten angezeigt werden, wird durch diesen Befehl auch eine Nachricht an `testaddr` gesendet. Nur ausgehende Mails können geprüft werden, ohne den `sendmail` -Service auf dem System neu zu starten. Bei Systemen, die noch keine Mails verwalten, verwenden Sie das vollständige Prüfverfahren, das unter „So prüfen Sie die Mailkonfiguration“ auf Seite 343 beschrieben ist.

7 Installieren Sie die neue Konfiguration, nachdem Sie eine Kopie des Originals erstellt haben.

```
# cp /etc/mail/sendmail.cf /etc/mail/sendmail.cf.save
# cp myhost.cf /etc/mail/sendmail.cf
```

8 Starten Sie den `sendmail`-Service neu.

```
# svcadm enable network/smtp:sendmail
```

Einrichten eines virtuellen Hosts

Wenn Sie einem Host mehrere IP-Adressen zuweisen müssen, informieren Sie sich auf der Website unter `http://www.sendmail.org/tips/virtualHosting`. Auf dieser Website finden Sie eine vollständige Anleitung, wie mithilfe von `sendmail` ein virtueller Host eingerichtet werden kann. Führen Sie jedoch im Abschnitt "Sendmail-Konfiguration" nicht den nachstehend aufgeführten Schritt 3b aus:

```
# cd sendmail-VERSION/cf/cf
# ./Build mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

Führen Sie stattdessen für das Betriebssystem Solaris die folgenden Schritte aus:

```
# cd /etc/mail/cf/cf
# /usr/ccs/bin/make mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

mailserver Verwenden Sie den Namen der `.cf`-Datei.

Unter „Ändern der sendmail-Konfiguration“ auf Seite 313 sind dieselben drei Schritte als Teil des Erstellungsverfahrens aufgeführt.

Nachdem Sie die `/etc/mail/sendmail.cf`-Datei erstellt haben, können Sie mit den nächsten Schritten fortfahren, um eine virtuelle Benutzertabelle zu erstellen.

▼ So konfigurieren Sie die automatische Neuerstellung einer Konfigurationsdatei

Wenn Sie eine eigene Kopie von `sendmail.cf` oder `submit.cf` erstellt haben, wird die Konfigurationsdatei während des Upgradeprozesses nicht ersetzt. Das folgende Verfahren

zeigt, wie die Eigenschaften des sendmail-Services konfiguriert werden, damit die Datei `sendmail.cf` automatisch für Sie neu erstellt wird. Informationen zum automatischen Erstellen der Konfigurationsdatei `submit.cf` finden Sie im Beispiel 13–1. Sie können diese Verfahren kombinieren, wenn Sie beide Dateien erstellen müssen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Legen Sie die sendmail-Eigenschaften fest.**

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/path_to_sendmail_mc=/etc/mail/cf/cf/myhost.mc
svc:/network/smtp:sendmail> quit
```

3. **Aktualisieren Sie den sendmail-Service, und starten Sie ihn neu.**

   Der erste Befehl überträgt die Änderungen in den ausgeführten Schnappschuss. Der zweite Befehl startet den sendmail-Service mithilfe der neuen Optionen neu.

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

Beispiel 13–1 Einrichten der automatischen Neuerstellung der Datei `submit.cf`

Mit diesem Verfahren wird der sendmail-Service so konfiguriert, dass die Konfigurationsdatei `submit.mc` automatisch neu erstellt wird.

```
# svccfg -s sendmail-client:default
svc:/network/smtp:sendmail> setprop config/path_to_submit_mc=/etc/mail/cf/cf/submit-myhost.mc
svc:/network/smtp:sendmail> exit
# svcadm refresh svc:/network/sendmail-client
# svcadm restart svc:/network/sendmail-client
```

▼ So verwenden Sie `sendmail` im offenen Modus

In der Version 10 von Solaris wurde der sendmail-Service geändert, sodass er standardmäßig im Modus "nur lokal" ausgeführt wird. Im Modus "nur lokal" werden nur Mails vom lokalen Host akzeptiert. Mails von anderen Systemen werden abgelehnt. Bei früheren Versionen von wurden alle von Remote-Systemen eingehenden Mails akzeptiert. Dies wurde als "offener Modus" bezeichnet. Um den offenen Modus zu verwenden, folgen Sie dem folgenden Verfahren.

Achtung – Das Ausführen von sendmail im Modus "nur lokal" ist viel sicherer als das Ausführen von sendmail im offenen Modus. Sie sollten die potenziellen Sicherheitsrisiken kennen, wenn Sie dieses Verfahren verwenden.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Legen Sie die sendmail-Eigenschaften fest.**

   ```
   # svccfg -s sendmail
   svc:/network/smtp:sendmail> setprop config/local_only = false
   svc:/network/smtp:sendmail> quit
   ```

3. **Aktualisieren Sie den sendmail-Service, und starten Sie ihn neu.**

   ```
   # svcadm refresh svc:/network/smtp:sendmail
   # svcadm restart svc:/network/smtp:sendmail
   ```

▼ So richten Sie SMTP zur Verwendung von TLS ein

Ab Version Solaris 10 1/06 hat SMTP die Möglichkeit, TLS (Transport Layer Security) in Version 8.13 von `sendmail` zu verwenden. Dieser Service für SMTP-Server und -Clients sorgt für eine verschlüsselte und authentifizierter Kommunikation über das Internet und für die Abwehr von Lausch- und Hackerangriffen. Beachten Sie, dass dieser Service nicht standardmäßig aktiviert ist.

Im folgenden Verfahren werden Beispieldaten verwendet, um zu veranschaulichen, wie Zertifikate eingerichtet werden, die `sendmail` ermöglichen, TLS zu verwenden. Weitere Informationen finden Sie unter „Unterstützung für die Ausführung von SMTP mit TLS in Version 8.13 von `sendmail`“ auf Seite 392.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Stoppen Sie `sendmail`.**

   ```
   # svcadm disable -t network/smtp:sendmail
   ```

3 Richten Sie die Zertifikate ein, die `sendmail` ermöglichen, TLS zu verwenden.

a. Führen Sie Folgendes aus:

```
# cd /etc/mail
# mkdir -p certs/CA
# cd certs/CA
# mkdir certs crl newcerts private
# echo "01" > serial
# cp /dev/null index.txt
# cp /etc/sfw/openssl/openssl.cnf .
```

b. Verwenden Sie den von Ihnen bevorzugten Texteditor, um den `dir`-Wert in der Datei `openssl.cnf` von `/etc/sfw/openssl` in `/etc/mail/certs/CA` zu ändern.

c. Verwenden Sie das `openssl`-Befehlszeilentool, um TLS zu implementieren.

Bitte beachten Sie, dass durch die folgende Befehlszeile interaktiver Text erstellt wird.

```
# openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
.....................................++++++
.....................................++++++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

`req`	Dieser Befehl erstellt und verarbeitet Zertifikatanforderungen.
`-new`	Diese `req`-Option erstellt eine neue Zertifikatanforderung.
`-x509`	Diese `req`-Option erstellt ein selbstsigniertes Zertifikat.
`-keyout private/cakey.pem`	Diese `req`-Option ermöglicht Ihnen, `private/cakey.pem` als Dateiname für den neu erstellten privaten Schlüssel zuzuweisen.

`-out cacert.pem`	Diese `req`-Option ermöglicht Ihnen, `cacert.pem` als Ihre Ausgabedatei zuzuweisen.
`-days 365`	Diese `req`-Option ermöglicht Ihnen, das Zertifikat für `365` Tage zu zertifizieren. Der Standardwert ist `30`.
`-config openssl.cnf`	Diese `req`-Option ermöglicht Ihnen, `openssl.cnf` als Konfigurationsdatei anzugeben.

Beachten Sie, dass Sie bei Verwendung dieses Befehls Folgendes angeben müssen:

- `Name des Landes`, beispielsweise `USA`
- `Name des Staates oder Bundeslands`, beispielsweise `Kalifornien`
- `Name des Ortes`, beispielsweise `Menlo Park`
- `Name des Unternehmens`, beispielsweise `Oracle Corporation`
- `Name der Organisationseinheit`, beispielsweise `Solaris`
- `Allgemeiner Name`: Dies ist der voll qualifizierte Hostname des Rechners. Weitere Informationen finden Sie auf der Manpage `check-hostname(1M)`.
- `Email Address`, beispielsweise `someuser@example.com`

4 (Optional) Wenn Sie eine neue sichere Verbindung benötigen, erstellen Sie ein neues Zertifikat und signieren es über die Zertifizierungsstelle.

a. Erstellen Sie ein neues Zertifikat.

```
# cd /etc/mail/certs/CA
# openssl req -nodes -new -x509 -keyout newreq.pem -out newreq.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
..............++++++
..............++++++
writing new private key to 'newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

Die Verwendung dieses Befehls erfordert, dass Sie dieselben Informationen wie in Schritt 3c bereitstellen.

Beachten Sie, dass sich das Zertifikat und der private Schlüssel in diesem Beispiel in der Datei `newreq.pem` befinden.

b. Signieren Sie das neue Zertifikat über die Zertifizierungsstelle.

```
# cd /etc/mail/certs/CA
# openssl x509 -x509toreq -in newreq.pem -signkey newreq.pem -out tmp.pem
Getting request Private Key
Generating certificate request
# openssl ca -config openssl.cnf -policy policy_anything -out newcert.pem -infiles tmp.pem
Using configuration from openssl.cnf
Enter pass phrase for /etc/mail/certs/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jun 23 18:44:38 2005 GMT
            Not After : Jun 23 18:44:38 2006 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            localityName              = Menlo Park
            organizationName          = Sun Microsystems
            organizationalUnitName    = Solaris
            commonName                = somehost.somedomain.example.com
            emailAddress              = someuser@example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                93:D4:1F:C3:36:50:C5:97:D7:5E:01:E4:E3:4B:5D:0B:1F:96:9C:E2
            X509v3 Authority Key Identifier:
                keyid:99:47:F7:17:CF:52:2A:74:A2:C0:13:38:20:6B:F1:B3:89:84:CC:68
                DirName:/C=US/ST=California/L=Menlo Park/O=Sun Microsystems/OU=Solaris/\
                CN=someuser@example.com/emailAddress=someuser@example.com
                serial:00

Certificate is to be certified until Jun 23 18:44:38 2006 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
# rm -f tmp.pem
```

In diesem Beispiel enthält die Datei `newreq.pem` das unsignierte Zertifikat und den privaten Schlüssel. Die Datei `newcert.pem` enthält das signierte Zertifikat.

`x509` utility	Zeigt Zertifikatinformationen an, konvertiert Zertifikate in verschiedene Formulare und signiert Zertifikatanforderungen.

ca application	Wird bei Anforderungen zum Signieren von Zertifikaten in vielfältigen Formularen und zum Erstellen von Zertifikat-Rücknahmelisten (Certificate Revocation Lists, CRL) verwendet.

5 Aktivieren Sie `sendmail`, um die Zertifikate zu verwenden, indem Sie die folgenden Zeilen in die `.mc`-Datei einfügen:

```
define('confCACERT_PATH', '/etc/mail/certs')dnl
define('confCACERT', '/etc/mail/certs/CAcert.pem')dnl
define('confSERVER_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confSERVER_KEY', '/etc/mail/certs/MYkey.pem')dnl
define('confCLIENT_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confCLIENT_KEY', '/etc/mail/certs/MYkey.pem')dnl
```

Weitere Informationen finden Sie unter „Konfigurationsdateioptionen zum Ausführen von SMTP mit TLS“ auf Seite 394.

6 Erstellen Sie die Datei `sendmail.cf` im `/etc/mail`-Verzeichnis neu, und installieren Sie sie.

Eine ausführliche Anleitung finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313.

7 Erstellen Sie symbolische Verknüpfungen, die von den Dateien, die Sie mit `openssl` erstellt haben, auf die Dateien verweisen, die Sie in der `.mc`-Datei definiert haben.

```
# cd /etc/mail/certs
# ln -s CA/cacert.pem CAcert.pem
# ln -s CA/newcert.pem MYcert.pem
# ln -s CA/newreq.pem MYkey.pem
```

8 Verweigern Sie Gruppen und anderen Benutzern die Leseberechtigung für `MYkey.pem`, um die Sicherheit zu erhöhen.

```
# chmod go-r MYkey.pem
```

9 Verwenden Sie eine symbolische Verknüpfung, um CA-Zertifikate in dem Verzeichnis zu installieren, das `confCACERT_PATH` zugewiesen ist.

```
# C=CAcert.pem
# ln -s $C 'openssl x509 -noout -hash < $C'.0
```

10 Um für eine sichere Übermittlung von Mails durch andere Hosts zu sorgen, installieren Sie die entsprechenden Hostzertifikate.

a. Kopieren Sie die Datei, die durch die Option `confCACERT` des anderen Hosts definiert wurde, in `/etc/mail/certs/`*host.domain*`.cert.pem`.

Ersetzen Sie *host.domain* durch den voll qualifizierten Hostnamen des anderen Hosts.

b. Verwenden Sie eine symbolische Verknüpfung, um CA-Zertifikate in dem Verzeichnis zu installieren, das `confCACERT_PATH` zugewiesen ist.

```
# C=host.domain.cert.pem
# ln -s $C 'openssl x509 -noout -hash < $C'.0
```

Ersetzen Sie *host.domain* durch den voll qualifizierten Hostnamen des anderen Hosts.

11 Starten Sie `sendmail` neu.

```
# svcadm enable network/smtp:sendmail
```

Beispiel 13–2 `Received:` Mail-Header

Es folgt ein Beispiel des Empfangs eines Mail-Headers (`Received:`) für die sichere Übermittlung von Mails mit TLS.

```
Received: from his.example.com ([IPv6:2001:db8:3c4d:15::1a2f:1a2b])
        by her.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNUB8i242496
        (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
        for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:11 -0800 (PST)
Received: from her.example.com (her.city.example.com [192.168.0.0])
        by his.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNU7cl571102
        version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
        for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:07 -0800 (PST)
```

Der Wert für `verify` ist `OK`, d. h., die Authentifizierung war erfolgreich. Weitere Informationen finden Sie unter „Makros zum Ausführen von SMTP mit TLS“ auf Seite 396.

Siehe auch Folgende OpenSSL Manpages:

- openssl(1) (`http://www.openssl.org/docs/apps/openssl.html`).
- req(1) (`http://www.openssl.org/docs/apps/req.html`).
- x509(1) (`http://www.openssl.org/docs/apps/x509.html`).
- ca(1) (`http://www.openssl.org/docs/apps/ca.html`).

▼ So verwalten Sie die Mailübermittlung mithilfe einer alternativen Konfiguration von `sendmail.cf`

Um die Übertragung von ein- und ausgehenden Mails zu vereinfachen, werden bei der neuen Standardkonfiguration von `sendmail` ein Dämon und ein Client-Warteschlangen-Betriebsprogramm verwendet. Durch das Client-Warteschlangen-Betriebsprogramm müssen Mails an den Dämon auf dem lokalen SMTP-Port weitergeleitet werden. Wenn der Dämon den SMTP-Port nicht überwacht, bleiben die Mails in der Warteschlange. Um dieses Problem zu vermeiden, führen Sie die folgende Aufgabe aus. Weitere Informationen zum Dämon, zum Client-Warteschlangen-Betriebsprogramm und zu den Gründen, warum Sie eventuell diese

alternative Konfiguration verwenden müssen, finden Sie unter „submit.cf-Konfigurationsdatei der Version 8.12 von sendmail“ auf Seite 401.

Mit diesem Verfahren wird sichergestellt, dass Ihr Dämon nur Verbindungen vom lokalen Host akzeptiert.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Stoppen Sie den `sendmail`-Client-Service.**

```
# svcadm disable -t sendmail-client
```

3 **Erstellen Sie eine Kopie der Konfigurationsdatei, die Sie ändern.**

```
# cd /etc/mail/cf/cf
# cp submit.mc submit-myhost.mc
```

myhost Legen Sie einen neuen Namen für Ihre `.mc`-Datei fest.

4 **Bearbeiten Sie die neue Konfigurationsdatei (beispielsweise `submit-` *myhost*`.mc`).**

Ändern Sie die IP-Adresse des empfangenden Hosts in der `msp`-Definition.

```
# grep msp submit-myhost.mc
FEATURE('msp', '[#.#.#.#]')dnl
```

5 **Erstellen Sie die Konfigurationsdatei mithilfe von `m4`.**

```
# /usr/ccs/bin/make submit-myhost.cf
```

6 **Installieren Sie die neue Konfiguration, nachdem Sie eine Kopie des Originals erstellt haben.**

```
# cp /etc/mail/submit.cf /etc/mail/submit.cf.save
# cp submit-myhost.cf /etc/mail/submit.cf
```

7 **Starten Sie den `sendmail`-Client-Service neu.**

```
# svcadm enable sendmail-client
```

Verwalten von Mailaliasdateien (Übersicht der Schritte)

In der folgenden Tabelle werden die Verfahren zum Verwalten von Mailaliasdateien beschrieben. Weitere Informationen zu diesem Thema finden Sie unter „Mail-Aliasdateien“ auf Seite 379 in Kapitel 14, „Mailservices (Referenz)“.

Aufgabe	Beschreibung	Siehe
Verwalten von Alias-Einträgen in einer NIS+-`mail_aliases`-Tabelle	Wenn es sich bei Ihrem Name Service um NIS+ handelt, verwenden Sie diese Verfahren, um die Inhalte Ihrer `mail_aliases`-Tabelle zu verwalten. Initiieren Sie eine NIS+-`mail_aliases`-Tabelle.	„So initiieren Sie eine NIS+-`mail_aliases`-Tabelle“ auf Seite 325
	Zeigen Sie die Inhalte der NIS+-`mail_aliases`-Tabelle in einer Liste an. Dieses Verfahren enthält Beispiele, die zeigen, wie einzelne Einträge und teilweise Entsprechungen aufgelistet werden.	„So listen Sie die Inhalte der NIS+-`mail_aliases`-Tabelle auf“ auf Seite 326
	Fügen Sie über die Befehlszeile Aliase in die NIS+-`mail_aliases`-Tabelle ein.	„So fügen Sie über die Befehlszeile Aliase in die NIS+-`mail_aliases`-Tabelle ein“ auf Seite 327
	Fügen Sie Einträge ein, indem Sie eine NIS+-`mail_aliases`-Tabelle bearbeiten.	„So fügen Sie Einträge durch Bearbeiten einer NIS+-`mail_aliases`-Tabelle ein“ auf Seite 328
	Bearbeiten Sie die Einträge in einer NIS+-`mail_aliases`-Tabelle. Dieses Verfahren enthält ein Beispiel, das zeigt, wie ein Eintrag gelöscht wird.	„So bearbeiten Sie Einträge in einer `mail_aliases`-NIS+-Tabelle“ auf Seite 329
Einrichten einer NIS-`mail.aliases`-Map	Wenn es sich bei Ihrem Name Service um NIS handelt, befolgen Sie diese Anweisungen, um das Aliasing mit einer `mail.aliases`-Map zu vereinfachen.	„So richten Sie eine `mail.aliases`-NIS-Map ein“ auf Seite 330
Einrichten einer lokalen Mailaliasdatei	Wenn Sie keinen Name Service (wie beispielsweise NIS oder NIS+) verwenden, befolgen Sie diese Anweisungen, um das Aliasing mit der `/etc/mail/aliases` -Datei zu vereinfachen.	„So richten Sie eine lokale Mailaliasdatei ein“ auf Seite 331
Erstellen einer verschlüsselten Zuordnungsdatei	Führen Sie diese Schritte aus, um das Aliasing mit einer verschlüsselten Zuordnungsdatei zu vereinfachen.	„So richten Sie eine verschlüsselte Zuordnungsdatei ein“ auf Seite 332
Einrichten des `postmaster`-Alias	Verwenden Sie die in diesem Abschnitt beschriebenen Verfahren, um den `postmaster`-Alias zu verwalten. Dieser Alias muss verfügbar sein.	„Verwalten des `postmaster`-Alias“ auf Seite 333

Verwalten von Mailaliasdateien

Mailaliase müssen innerhalb der Domain eindeutig sein. Dieser Abschnitt enthält die Verfahren zum Verwalten von Mailaliasdateien. Sie können auch die Mailing-Listen-Funktion in der Solaris Management Console verwenden, um diese Aufgaben für die Alias-Datenbank auszuführen.

Außerdem können Sie mithilfe von `makemap` Datenbankdateien für den lokalen Mailhost erstellen. Weitere Informationen finden Sie auf der Manpage `makemap(1M)`. Die Verwendung dieser Datenbankdateien bietet nicht alle Vorteile eines Name Service (z. B. NIS oder NIS+). Sie sollten jedoch die Daten aus diesen lokalen Datenbankdateien schneller abrufen können, weil keine Suche im Netzwerk stattfindet. Weitere Informationen finden Sie unter „Interaktionen von `sendmail` mit Name Services“ auf Seite 386 und „Mail-Aliasdateien“ auf Seite 379 in Kapitel 14, „Mailservices (Referenz)“.

Wählen Sie eines der folgenden Verfahren:

- „So initiieren Sie eine NIS+-`mail_aliases`-Tabelle“ auf Seite 325
- „So listen Sie die Inhalte der NIS+-`mail_aliases`-Tabelle auf“ auf Seite 326
- „So fügen Sie über die Befehlszeile Aliase in die NIS+-`mail_aliases`-Tabelle ein“ auf Seite 327
- „So fügen Sie Einträge durch Bearbeiten einer NIS+-`mail_aliases`-Tabelle ein“ auf Seite 328
- „So bearbeiten Sie Einträge in einer `mail_aliases`-NIS+-Tabelle“ auf Seite 329
- „So richten Sie eine `mail.aliases`-NIS-Map ein“ auf Seite 330
- „So richten Sie eine lokale Mailaliasdatei ein“ auf Seite 331
- „So richten Sie eine verschlüsselte Zuordnungsdatei ein“ auf Seite 332

▼ So initiieren Sie eine NIS+-`mail_aliases`-Tabelle

Sie können den Befehl `aliasadm` verwenden, um die Einträge in einer NIS+-Tabelle zu verwalten. Um eine Tabelle zu erstellen, befolgen Sie diese Anweisungen. Weitere Informationen finden Sie auf der Manpage `aliasadm(1M)`.

1. **Werden Sie entweder ein Mitglied der NIS+-Gruppe, die im Besitz der Tabelle ist, oder melden Sie sich als `Root` beim Mailserver oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Initiieren Sie eine NIS+-Tabelle.**

   ```
   # aliasadm -I
   ```

3. **Fügen Sie Einträge in die Tabelle ein.**

- Informationen zum Einfügen von zwei oder drei Aliasen finden Sie unter „So fügen Sie über die Befehlszeile Aliase in die NIS+-mail_aliases-Tabelle ein“ auf Seite 327.
- Informationen zum Einfügen von mehr als zwei oder drei Aliasen finden Sie unter „So fügen Sie Einträge durch Bearbeiten einer NIS+-mail_aliases-Tabelle ein“ auf Seite 328.

So listen Sie die Inhalte der NIS+-mail_aliases-Tabelle auf

Um eine vollständige Liste der Tabelleninhalte anzuzeigen, befolgen Sie diese Anweisungen.

1 **Werden Sie entweder ein Mitglied der NIS+-Gruppe, die im Besitz der Tabelle ist, oder melden Sie sich als Root beim Mailmerver oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Listen Sie alle Einträge in alphabetischer Reihenfolge nach Alias auf.**

```
# aliasadm -1
```

Weitere Informationen finden Sie auf der Manpage aliasadm(1M).

Beispiel 13–3 Auflisten eines einzelnen Eintrags aus der NIS+-mail_aliases-Tabelle

Zum Auflisten von einzelnen Einträgen können Sie auch den Befehl aliasadm verwenden. Nachdem Sie den ersten Schritt dieses Verfahrens ausgeführt haben, geben Sie Folgendes ein:

```
# aliasadm -m ignatz
ignatz: ignatz@saturn # Alias for Iggy Ignatz
```

Der Befehl gleicht nur den vollständigen Aliasnamen ab, aber keine Teile von Zeichenfolgen. Sie können keine Metazeichen wie beispielsweise * und ? zusammen mit aliasadm -m verwenden.

Beispiel 13–4 Auflisten von teilweisen Entsprechungen aus der NIS+-mail_aliases-Tabelle

Zum Auflisten von teilweisen Entsprechungen können Sie auch den Befehl aliasadm verwenden. Nachdem Sie den ersten Schritt dieses Verfahrens ausgeführt haben, geben Sie Folgendes ein:

```
# aliasadm -l | grep partial-string
```

Ersetzen Sie *partial-string* durch die Zeichenfolge, die Sie für die Suche verwenden.

▼ So fügen Sie über die Befehlszeile Aliase in die NIS+-`mail_aliases`-Tabelle ein

Um zwei oder drei Aliase in die Tabelle einzufügen, befolgen Sie diese Anweisungen. Informationen zum Einfügen von mehr als zwei oder drei Aliasen finden Sie unter „So fügen Sie Einträge durch Bearbeiten einer NIS+-`mail_aliases`-Tabelle ein“ auf Seite 328.

1. **Stellen Sie Listen zusammen, in denen die jeweiligen Mailclients, die Adressen der zugehörigen Mailboxen und die Namen der Mailserversysteme enthalten sind.**

2. **Werden Sie entweder ein Mitglied der NIS+-Gruppe, die im Besitz der Tabelle ist, oder melden Sie sich als `Root` beim Mailserver oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

3. **(Optional) Initiieren Sie bei Bedarf eine NIS+-Tabelle.**

   Um eine völlig neue NIS+-`mail_aliases` -Tabelle zu erstellen, müssen Sie die Tabelle zunächst initiieren. Aufgabenbezogene Informationen finden Sie unter „So initiieren Sie eine NIS+-`mail_aliases`-Tabelle“ auf Seite 325.

4. **Fügen Sie Aliase in die Tabelle ein.**

   In diesem Beispiel wird ein typischer Eintrag gezeigt.

   ```
   # aliasadm -a iggy iggy.ignatz@saturn "Iggy Ignatz"
   ```

   In der folgenden Liste werden die Teile des Eintrags aus dem vorangegangenen Beispiel beschrieben.

`-a`	die Option zum Hinzufügen eines Alias
`iggy`	die Kurzform des Aliasnamens
`iggy.ignatz@saturn`	der erweiterte Aliasname
`"Iggy Ignatz"`	der Name des Alias in Anführungszeichen

5. **Zeigen Sie den von Ihnen erstellten Eintrag an, und stellen Sie sicher, dass der Eintrag korrekt ist.**

   `# aliasadm -m` *alias*

   alias der von Ihnen erstellte Eintrag

   Weitere Informationen finden Sie auf der Manpage `aliasadm(1M)`.

▼ So fügen Sie Einträge durch Bearbeiten einer NIS+-`mail_aliases`-Tabelle ein

Sie können den Befehl `aliasadm` verwenden, um die Einträge in einer NIS+-Tabelle zu verwalten. Um mehr als zwei oder drei Aliase in die Tabelle einzufügen, befolgen Sie diese Anweisungen.

1 Stellen Sie Listen zusammen, in denen die jeweiligen Mailclients, die Adressen der zugehörigen Mailboxen und die Namen der Mail-Server-Systeme enthalten sind.

2 Werden Sie entweder ein Mitglied der NIS+-Gruppe, die im Besitz der Tabelle ist, oder melden Sie sich als `Root` beim Mailserver oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

3 Zeigen Sie die Alias-Tabelle an, und bearbeiten Sie sie.

```
# aliasadm -e
```

Mithilfe dieses Befehls können Sie die Tabelle anzeigen und bearbeiten. Der Editor, den Sie verwenden, wurde mit der Umgebungsvariablen `$EDITOR` definiert. Wenn diese Variable nicht definiert ist, ist `vi` der Standard-Editor.

4 Verwenden Sie das folgende Format, um jeden Alias in eine separate Zeile einzutragen.

alias`:` *expanded-alias* `#` `[`"*option*" `#` "*comments*"`]`

alias	Diese Spalte ist für die Kurzform des Aliasnamens vorgesehen.
expanded-alias	Diese Spalte ist für den erweiterten Aliasnamen vorgesehen.
option	Diese Spalte ist für die spätere Verwendung reserviert.
comments	Diese Spalte wird für Kommentare zum jeweiligen Alias verwendet, beispielsweise zu einem Aliasnamen.

Wenn Sie die Optionsspalte leer lassen, geben Sie Anführungszeichen ein, in denen nichts eingeschlossen ist (`""`). Anschließend geben Sie die Kommentare ein.

Die Reihenfolge der Einträge ist für die NIS+-`mail_aliases` -Tabelle nicht von Bedeutung. Mit dem Befehl `aliasadm -l` werden die Listen sortiert und in alphabetischer Reihenfolge angezeigt.

Weitere Informationen finden Sie unter „Mail-Aliasdateien“ auf Seite 379 und auf der Manpage `aliasadm(1M)`.

▼ So bearbeiten Sie Einträge in einer `mail_aliases`-NIS+-Tabelle

Um Einträge in der Tabelle zu bearbeiten, befolgen Sie die nachstehenden Anweisungen.

1 **Werden Sie entweder ein Mitglied der NIS+-Gruppe, die im Besitz der Tabelle ist, oder melden Sie sich als `Root` beim Mailserver oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Zeigen Sie den Aliaseintrag an.**

```
# aliasadm -m alias
```

Ersetzen Sie *alias* durch den zugewiesenen Aliasnamen.

3 **Bearbeiten Sie nach Bedarf den Aliaseintrag.**

```
# aliasadm -c alias expanded-alias [options comments]
```

alias	Bearbeiten Sie nach Bedarf den Aliasnamen.
expanded-alias	Bearbeiten Sie nach Bedarf den erweiterten Aliasnamen.
options	Bearbeiten Sie nach Bedarf die Option.
comments	Bearbeiten Sie nach Bedarf den Kommentar für diesen Eintrag.

Weitere Informationen finden Sie auf der Manpage `aliasadm`(1M) sowie unter „Mail-Aliasdateien“ auf Seite 379.

4 **Zeigen Sie den von Ihnen bearbeiteten Eintrag an, und stellen Sie sicher, dass der Eintrag korrekt ist.**

```
# aliasadm -m alias
```

Weitere Informationen finden Sie auf der Manpage `aliasadm`(1M).

Beispiel 13–5 Löschen von Einträgen aus einer NIS+-`mail_aliases`-Tabelle

Um Einträge aus der Tabelle zu löschen, verwenden Sie die folgende Syntax, nachdem Sie den ersten Schritt in diesem Verfahren ausgeführt haben:

```
# aliasadm -d alias
```

Ersetzen Sie *alias* durch den Aliasnamen für den Eintrag, den Sie löschen.

▼ So richten Sie eine `mail.aliases`-NIS-Map ein

Verwenden Sie das folgende Verfahren, um das Aliasing mit einer `mail.aliases`-NIS-Map zu vereinfachen.

1 **Stellen Sie Listen zusammen, in denen die jeweiligen Mailclients, die Adressen der zugehörigen Mailboxen und die Namen der Mailserversysteme enthalten sind.**

2 **Melden Sie sich als `Root` beim NIS-Master-Server oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

3 **Bearbeiten Sie die Datei `/etc/mail/aliases`, und fügen Sie die folgenden Einträge hinzu.**

a. **Fügen Sie einen Eintrag für jeden Mailclient hinzu.**

```
# cat /etc/mail/aliases
..
alias:expanded-alias
```

alias — Verwenden Sie den kurzen Aliasnamen.

expanded-alias — Verwenden Sie den erweiterten Aliasnamen (`user@host.domain.com`).

b. **Stellen Sie sicher, dass Sie über einen `Postmaster: root`-Eintrag verfügen.**

```
# cat /etc/mail/aliases
..
Postmaster: root
```

c. **Fügen Sie ein Alias für `root` hinzu. Verwenden Sie die Mailadresse der Person, die als Postmaster benannt ist.**

```
# cat /etc/mail/aliases
..
root: user@host.domain.com
```

user@host.domain.com — Verwenden Sie die zugewiesene Adresse des benannten Postmasters.

4 **Stellen Sie sicher, dass der NIS-Master-Server als Name Service ausgeführt wird, um die Hostnamen auf jedem Mailserver aufzulösen.**

5 **Wechseln Sie in das Verzeichnis `/var/yp`.**

```
# cd /var/yp
```

6 **Führen Sie den Befehl `make` aus.**

```
# make
```

Die Änderungen in den Dateien `/etc/hosts` und `/etc/mail/aliases` werden in die NIS-Slave-Systeme übertragen. Die Änderungen werden meist nach nur wenigen Minuten wirksam.

▼ So richten Sie eine lokale Mailaliasdatei ein

Verwenden Sie das folgende Verfahren, um Aliase mit einer lokalen Aliasdatei aufzulösen.

1 **Stellen Sie Listen zusammen, in denen Ihre Benutzer und die Adressen der zugehörigen Mailboxen enthalten sind.**

2 **Melden Sie sich als `Root` beim Mailserver oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

3 **Bearbeiten Sie die Datei `/etc/mail/aliases`, und fügen Sie die folgenden Einträge hinzu.**

a. **Fügen Sie einen Eintrag für jeden Benutzer hinzu.**

user1`:` *user2@host.domain*

user1	Verwenden Sie den neuen Aliasnamen.
user2@host.domain	Verwenden Sie die aktuelle Adresse für den neuen Alias.

b. **Stellen Sie sicher, dass Sie über einen `Postmaster: root`-Eintrag verfügen.**

```
# cat /etc/mail/aliases
..
Postmaster: root
```

c. **Fügen Sie ein Alias für `root` hinzu. Verwenden Sie die Mailadresse der Person, die als Postmaster benannt ist.**

```
# cat /etc/mail/aliases
..
root: user@host.domain.com
```

user@host.domain.com	Verwenden Sie die zugewiesene Adresse des benannten Postmasters.

4 **Erstellen Sie die Alias-Datenbank neu.**

```
# newaliases
```

Mit der Konfiguration der `AliasFile`-Option in `/etc/mail/sendmail.cf` wird festgelegt, ob mit diesem Befehl entweder eine einzelne Datei (`/etc/mail/aliases.db`) oder ein Paar von Dateien (`/etc/mail/aliases.dir` und `/etc/mail/aliases.pag`) in binärer Form erstellt wird.

5 Führen Sie einen der folgenden Schritte aus, um die erstellte Datei bzw. die erstellten Dateien zu kopieren.

a. (Optional) Kopieren Sie die Dateien `/etc/mail/aliases`, `/etc/mail/aliases.dir` und die `/etc/mail/aliases.pag` in die jeweils anderen Systeme.

Sie können die drei Dateien mit dem Befehl `rcp` oder mit dem Befehl `rdist` kopieren. Weitere Informationen finden Sie auf der Manpage `rcp(1)` oder der Manpage `rdist(1)`. Sie können auch ein Skript zu diesem Zweck erstellen.

Wenn Sie diese Dateien kopieren, müssen Sie den Befehl `newaliases` nicht für jedes der anderen Systeme ausführen. Beachten Sie jedoch, dass Sie jedesmal dann, wenn Sie einen Mailclient hinzufügen oder entfernen, alle `/etc/mail/aliases`-Dateien aktualisieren müssen.

b. (Optional) Kopieren Sie die `/etc/mail/aliases`-Datei und die `/etc/mail/aliases.db`-Datei in jedes der anderen Systeme.

Sie können diese Dateien mit dem Befehl `rcp` oder mit dem Befehl `rdist` kopieren. Weitere Informationen finden Sie auf der Manpage `rcp(1)` oder der Manpage `rdist(1)`. Sie können auch ein Skript zu diesem Zweck erstellen.

Wenn Sie diese Dateien kopieren, müssen Sie den Befehl `newaliases` nicht für jedes der anderen Systeme ausführen. Beachten Sie jedoch, dass Sie jedesmal dann, wenn Sie einen Mailclient hinzufügen oder entfernen, alle `/etc/mail/aliases`-Dateien aktualisieren müssen.

▼ So richten Sie eine verschlüsselte Zuordnungsdatei ein

Um eine verschlüsselte Zuordnungsdatei zu erstellen, befolgen Sie diese Anweisungen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Erstellen Sie eine Eingabedatei.

Einträge können die folgende Syntax aufweisen:

```
old-name@newdomain.com     new-name@newdomain.com
old-name@olddomain.com     error:nouser No such user here
@olddomain.com             %1@newdomain.com
```

old_name@newdomain.com	Verwenden Sie den Benutzernamen, der zuvor mit der neu zugewiesenen Domain zugewiesen wurde.
new_name@newdomain.com	Verwenden Sie die neu zugewiesene Adresse.
old_name@olddomain.com	Verwenden Sie den Benutzernamen, der bereits mit der zuvor zugewiesenen Domain zugewiesen wurde.
olddomain.com	Verwenden Sie die zuvor zugewiesene Domain.
newdomain.com	Verwenden Sie die neu zugewiesene Domain.

Der erste Eintrag leitet Mails an den neuen Alias weiter. Der nächste Eintrag erstellt eine Meldung, wenn ein falscher Alias verwendet wird. Der letzte Eintrag leitet alle von `olddomain` eingehenden Mails an `newdomain` weiter.

3 Erstellen Sie die Datenbankdatei.

```
# /usr/sbin/makemap maptype newmap < newmap
```

maptype	Wählen Sie einen Datenbanktyp wie beispielsweise `dbm`, `btree` oder `hash`.
newmap	Verwenden Sie den Namen der Eingabedatei und den ersten Teil des Namens der Datenbankdatei. Wenn der Datenbanktyp `dbm` ausgewählt wird, werden die Datenbankdateien mithilfe der Suffixe `.pag` und `.dir` erstellt. Bei den anderen beiden Datenbanktypen folgt dem Dateinamen das Suffix `.db`.

Verwalten des `postmaster`-Alias

Jedes System muss Mails an die `postmaster` -Mailbox senden können. Sie können ein NIS- oder NIS+-Alias für `postmaster` oder ein Alias in jeder lokalen `/etc/mail/aliases`-Datei erstellen. Relevante Informationen finden Sie unter:

- „So erstellen Sie ein `postmaster`-Alias in jeder lokalen `/etc/mail/aliases`-Datei“ auf Seite 334
- „So erstellen Sie eine separate Mailbox für `postmaster`“ auf Seite 334
- „So fügen Sie die `postmaster`-Mailbox den Aliasen in der `/etc/mail/aliases`-Datei hinzu“ auf Seite 335

So erstellen Sie ein `postmaster`-Alias in jeder lokalen `/etc/mail/aliases`-Datei

Wenn Sie das `postmaster`-Alias in jeder lokalen `/etc/mail/aliases`-Datei erstellen, befolgen Sie die nachstehenden Anweisungen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Zeigen Sie den `/etc/mail/aliases`-Eintrag an.**

   ```
   # cat /etc/mail/aliases
   # Following alias is required by the mail protocol, RFC 2821
   # Set it to the address of a HUMAN who deals with this system's
   # mail problems.
   Postmaster: root
   ```

3. **Bearbeiten Sie die `/etc/mail/aliases` -Datei jedes Systems.**

   Ändern Sie `root` in die Mailadresse der Person, die als Postmaster benannt ist.

   `Postmaster:` *mail-address*

   mail-address Verwenden Sie die zugewiesene Adresse der Person, die als Postmaster benannt ist.

4. **(Optional) Erstellen Sie eine separate Mailbox für den Postmaster.**

   Sie können eine separate Mailbox für den Postmaster erstellen, um die Postmaster-Mails von persönlichen Mails zu trennen. Wenn Sie eine separate Mailbox erstellen, verwenden Sie die Mailbox-Adresse anstelle der persönlichen Mailadresse des Postmasters, um die `/etc/mail/aliases`-Dateien zu bearbeiten. Weitere Informationen finden Sie unter „So erstellen Sie eine separate Mailbox für `postmaster`“ auf Seite 334.

So erstellen Sie eine separate Mailbox für `postmaster`

Wenn Sie eine separate Mailbox für `postmaster` erstellen, befolgen Sie die nachstehenden Anweisungen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erstellen Sie ein Benutzerkonto für die Person, die als `Postmaster` benannt ist. Tragen Sie ein Sternchen (*) in das Passwortfeld ein.**

   Weitere Informationen zum Hinzufügen eines Benutzerkontos finden Sie in „Setting Up User Accounts (Task Map)“ in *System Administration Guide: Basic Administration*.

3. **Nach der Mailübermittlung aktivieren Sie das `mail`-Programm, um den Namen der Mailbox lesen und beschreiben zu können.**

   ```
   # mail -f postmaster
   ```

   postmaster Verwenden Sie die zugewiesene Adresse.

▼ So fügen Sie die `postmaster`-Mailbox den Aliasen in der `/etc/mail/aliases`-Datei hinzu

Wenn Sie eine `postmaster`-Mailbox den Aliasen in der `/etc/mail/aliases`-Datei hinzufügen, befolgen Sie die nachstehenden Anweisungen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Fügen Sie ein Alias für `root` hinzu. Verwenden Sie die Mailadresse der Person, die als Postmaster benannt ist.**

   ```
   # cat /etc/mail/aliases
   ..
   root: user@host.domain.com
   ```

   user@host.domain.com Verwenden Sie die zugewiesene Adresse der Person, die als Postmaster benannt ist.

3. **Erstellen Sie auf dem lokalen System des Postmasters einen Eintrag in der `/etc/mail/aliases`-Datei, die den Namen des Alias definiert. `sysadmin` ist ein Beispiel. Geben Sie auch den Pfad zur lokalen Mailbox an.**

   ```
   # cat /etc/mail/aliases
   ..
   sysadmin: /usr/somewhere/somefile
   ```

   sysadmin Erstellen Sie einen Namen für einen neuen Alias.

   /usr/somewhere/somefile Verwenden Sie den Pfad zur lokalen Mailbox.

4. **Erstellen Sie die Alias-Datenbank neu.**

   ```
   # newaliases
   ```

Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)

In der nachstehenden Tabelle werden die Verfahren zum Verwalten der Mailwarteschlange beschrieben.

Aufgabe	Beschreibung	Anweisungen
Anzeigen des Inhalts der Mailwarteschlange (`/var/spool/mqueue`)	Wenden Sie dieses Verfahren an, um anzuzeigen, wie viele Mails in der Warteschlange stehen und wie schnell die Mails aus der Warteschlange entfernt werden.	„So zeigen Sie den Inhalt der Mailwarteschlange (`/var/spool/mqueue`) an“ auf Seite 337
Erzwingen der Verarbeitung der Mailwarteschlange (`/var/spool/mqueue`)	Wenden Sie dieses Verfahren an, um Mails für ein System zu verarbeiten, das zuvor keine Mails empfangen konnte.	„So erzwingen Sie die Verarbeitung der Mailwarteschlange (`/var/spool/mqueue`)“ auf Seite 337
Ausführen eines Teils der Mailwarteschlange (`/var/spool/mqueue`)	Wenden Sie dieses Verfahren an, um die Verarbeitung eines Teils einer Adresse (wie beispielsweise eines Hostnamens) zu erzwingen. Auch können Sie dieses Verfahren verwenden, um die Verarbeitung einer bestimmten Mail aus der Warteschlange zu erzwingen.	„So führen Sie einen Teil der Mailwarteschlange (`/var/spool/mqueue`) aus“ auf Seite 338
Verschieben der Mailwarteschlange (`/var/spool/mqueue`)	Wenden Sie dieses Verfahren an, um die Mailwarteschlange zu verschieben.	„So verschieben Sie die Mailwarteschlange (`/var/spool/mqueue`)“ auf Seite 338
Ausführen der alten Mailwarteschlange (`/var/spool/omqueue`)	Wenden Sie dieses Verfahren an, um eine alte Mailwarteschlange auszuführen.	„So führen Sie die alte Mailwarteschlange (`/var/spool/omqueue`) aus“ auf Seite 339

Verwalten der Warteschlangenverzeichnisse

In diesem Abschnitt werden hilfreiche Aufgaben für die Verwaltung von Warteschlangen beschrieben. Weitere Informationen zur ausschließlich für Clients reservierten Warteschlange finden Sie unter „`submit.cf`-Konfigurationsdatei der Version 8.12 von `sendmail`“ auf Seite 401. Weitere relevante Informationen finden Sie unter „Zusätzliche Warteschlangenfunktionen ab Version 8.12 von `sendmail`“ auf Seite 414.

Relevante Informationen finden Sie unter:

- „So zeigen Sie den Inhalt der Mailwarteschlange (`/var/spool/mqueue`) an“ auf Seite 337
- „So erzwingen Sie die Verarbeitung der Mailwarteschlange (`/var/spool/mqueue`)“ auf Seite 337
- „So führen Sie einen Teil der Mailwarteschlange (`/var/spool/mqueue`) aus“ auf Seite 338
- „So verschieben Sie die Mailwarteschlange (`/var/spool/mqueue`)“ auf Seite 338

- „So führen Sie die alte Mailwarteschlange (/var/spool/omqueue) aus“ auf Seite 339

So zeigen Sie den Inhalt der Mailwarteschlange (/var/spool/mqueue) an

- **Zeigen Sie an, wie viele Mails in der Warteschlange stehen und wie schnell die Mails aus der Warteschlange entfernt werden.**

  Geben Sie Folgendes ein:

  ```
  # /usr/bin/mailq | more
  ```

  Dieser Befehl stellt folgende Informationen bereit:

  - die Warteschlangen-IDs
  - die Größe der Mail
  - das Datum, an dem die Mail in die Warteschlange gestellt wurde
  - den Status der Mail
  - den Sender und die Empfänger

  Außerdem überprüft dieser Befehl jetzt das Autorisierungsattribut (`solaris.admin.mail.mailq`). Bei erfolgreicher Prüfung wird das Äquivalent des angegebenen `-bp`-Flag mit `sendmail` ausgeführt. Bei nicht erfolgreicher Prüfung wird eine Fehlermeldung ausgegeben. Das Autorisierungsattribut ist standardmäßig für alle Benutzer aktiviert. Das Autorisierungsattribut kann deaktiviert werden, indem der Benutzereintrag in `prof_attr` geändert wird. Weitere Informationen finden Sie auf der Manpage für `prof_attr(4)` und `mailq(1)`.

So erzwingen Sie die Verarbeitung der Mailwarteschlange (/var/spool/mqueue)

Wenden Sie dieses Verfahren an, um beispielsweise Mails für ein System zu verarbeiten, das zuvor keine Mails empfangen konnte.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erzwingen Sie die Verarbeitung einer Warteschlange, und zeigen Sie den Fortschritt der Jobs an, während die Warteschlange geleert wird.**

   ```
   # /usr/lib/sendmail -q -v
   ```

▼ So führen Sie einen Teil der Mailwarteschlange (`/var/spool/mqueue`) aus

Wenden Sie dieses Verfahren an, um beispielsweise die Verarbeitung eines Teils einer Adresse (wie beispielsweise eines Hostnamens) zu erzwingen. Auch können Sie dieses Verfahren verwenden, um die Verarbeitung einer bestimmten Mail aus der Warteschlange zu erzwingen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Mit `-qR`*string* können Sie jederzeit einen Teil der Mailwarteschlange ausführen.

```
# /usr/lib/sendmail -qRstring
```

string Verwenden Sie den Alias eines Empfängers oder einen Teil von *user@host.domain* , beispielsweise als Hostname.

Sie können auch einen Teil der Mailwarteschlange mit `-qI` *nnnnn* ausführen.

```
# /usr/lib/sendmail -qInnnnn
```

nnnnn Verwenden Sie eine Warteschlangen-ID.

▼ So verschieben Sie die Mailwarteschlange (`/var/spool/mqueue`)

Um die Mailwarteschlange zu verschieben, befolgen Sie die nachstehenden Anweisungen.

1 Melden Sie sich als `Root` beim Mailhost oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Brechen Sie den `sendmail`-Dämon ab.

```
# svcadm disable network/smtp:sendmail
```

Jetzt wird das Warteschlangenverzeichnis nicht mehr von `sendmail` verarbeitet.

3 Wechseln Sie in das Verzeichnis `/var/spool`.

```
# cd /var/spool
```

4. **Verschieben Sie das Verzeichnis mqueue und seinen gesamten Inhalt in das Verzeichnis omqueue. Dann erstellen Sie ein neues (leeres) Verzeichnis namens mqueue.**

   ```
   # mv mqueue omqueue; mkdir mqueue
   ```

5. **Setzen Sie die Berechtigungen des Verzeichnisses auf die Option zum Lesen/Schreiben/Ausführen durch den Eigentümer und Lesen/Schreiben/Ausführen durch eine Gruppe. Setzen Sie zudem den Eigentümer und die Gruppe auf daemon.**

   ```
   # chmod 750 mqueue; chown root:bin mqueue
   ```

6. **Starten Sie sendmail.**

   ```
   # svcadm enable network/smtp:sendmail
   ```

▼ So führen Sie die alte Mailwarteschlange (/var/spool/omqueue) aus

Um eine alte Mailwarteschlange auszuführen, befolgen Sie die nachstehenden Anweisungen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Führen Sie die alte Mailwarteschlange aus.**

   ```
   # /usr/lib/sendmail -oQ/var/spool/omqueue -q
   ```

   Das Flag -oQ gibt ein alternatives Warteschlangenverzeichnis an. Das Flag -q gibt an, dass jeder Job in der Warteschlange ausgeführt werden soll. Verwenden Sie das Flag -v, wenn Sie die ausführliche Ausgabe auf dem Bildschirm anzeigen.

3. **Entfernen Sie das leere Verzeichnis.**

   ```
   # rmdir /var/spool/omqueue
   ```

Verwalten von .forward-Dateien (Übersicht der Schritte)

In der folgenden Tabelle sind die Verfahren zum Verwalten von .forward-Dateien beschrieben. Weitere Informationen finden Sie unter „.forward-Dateien“ auf Seite 382 in Kapitel 14, „Mailservices (Referenz)“.

Aufgabe	Beschreibung	Siehe
Deaktivieren von .forward-Dateien	Wenden Sie dieses Verfahren an, wenn Sie beispielsweise automatische Weiterleitung verhindern möchten.	„So deaktivieren Sie .forward-Dateien“ auf Seite 340
Ändern des .forward-Dateisuchpfads	Wenden Sie dieses Verfahren an, wenn Sie beispielsweise alle .forward-Dateien in ein allgemeines Verzeichnis verschieben möchten.	„So ändern Sie den .forward-Dateisuchpfad“ auf Seite 341
Erstellen und Auffüllen von /etc/shells	Wenden Sie dieses Verfahren an, um Benutzern zu ermöglichen, mithilfe der .forward-Datei Mails an ein Programm oder eine Datei weiterzuleiten.	„So erstellen und füllen Sie /etc/shells“ auf Seite 342

Verwalten von .forward-Dateien

Dieser Abschnitt enthält verschiedene Verfahren im Zusammenhang mit der Verwaltung von .forward-Dateien. Da diese Dateien von Benutzern bearbeitet werden können, können sie Probleme verursachen. Weitere Informationen finden Sie unter „.forward-Dateien“ auf Seite 382 in Kapitel 14, „Mailservices (Referenz)“.

Relevante Informationen finden Sie unter:

- „So deaktivieren Sie .forward-Dateien“ auf Seite 340
- „So ändern Sie den .forward-Dateisuchpfad“ auf Seite 341
- „So erstellen und füllen Sie /etc/shells“ auf Seite 342

▼ So deaktivieren Sie .forward-Dateien

Mithilfe dieses Verfahrens wird die automatische Weiterleitung verhindert und die .forward-Datei für einen bestimmten Host deaktiviert.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Erstellen Sie eine Kopie von /etc/mail/cf/domain/solaris-generic.m4 oder von Ihrer m4-Datei der standortspezifischen Domain.

```
# cd /etc/mail/cf/domain
# cp solaris-generic.m4 mydomain.m4
```

mydomain Verwenden Sie einen Dateinamen Ihrer Wahl.

3. **Fügen Sie die folgende Zeile in die Datei ein, die Sie gerade erstellt haben.**

   ```
   define('confFORWARD_PATH','')dnl
   ```

   Wenn für confFORWARD_PATH in der m4-Datei bereits ein Wert vorhanden ist, ersetzen Sie den Wert durch diesen Nullwert.

4. **Erstellen und installieren Sie eine neue Konfigurationsdatei.**

   Die notwendigen Informationen dazu finden Sie unter „So erstellen Sie eine neue sendmail.cf-Datei“ auf Seite 314.

Hinweis – Wenn Sie die .mc-Datei bearbeiten, sollten Sie DOMAIN('solaris-generic') in DOMAIN('*mydomain* ') ändern.

▼ So ändern Sie den .forward-Dateisuchpfad

Wenn Sie beispielsweise alle .forward-Dateien in ein allgemeines Verzeichnis verschieben möchten, befolgen Sie die nachstehenden Anweisungen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erstellen Sie eine Kopie von /etc/mail/cf/domain/solaris-generic.m4 oder von Ihrer m4-Datei der standortspezifischen Domain.**

   ```
   # cd /etc/mail/cf/domain
   # cp solaris-generic.m4 mydomain.m4
   ```

   mydomain Verwenden Sie einen Dateinamen Ihrer Wahl.

3. **Fügen Sie die folgende Zeile in die Datei ein, die Sie gerade erstellt haben.**

   ```
   define('confFORWARD_PATH','$z/.forward:/var/forward/$u')dnl
   ```

   Wenn für confFORWARD_PATH in der m4 bereits ein Wert vorhanden ist, ersetzen Sie den Wert durch diesen neuen Wert.

4. **Erstellen und installieren Sie eine neue Konfigurationsdatei.**

   Die notwendigen Informationen dazu finden Sie unter „So erstellen Sie eine neue sendmail.cf-Datei“ auf Seite 314.

Hinweis – Wenn Sie die .mc-Datei bearbeiten, sollten Sie DOMAIN('solaris-generic') in DOMAIN('*mydomain* ') ändern.

▼ So erstellen und füllen Sie `/etc/shells`

Diese Datei ist nicht in der Standardversion enthalten. Sie müssen die Datei hinzufügen, wenn den Benutzern gestattet werden soll, mithilfe der `.forward`-Dateien Mails an ein Programm oder an eine Datei weiterzuleiten. Sie können die Datei manuell erstellen, indem Sie `grep` verwenden, um alle Shells zu ermitteln, die in Ihrer Passwortdatei aufgelistet sind. Anschließend können Sie die Shells in die Datei eintragen. Das folgende Verfahren, bei dem ein herunterladbares Skript verwendet wird, ist jedoch einfacher in der Durchführung.

1. **Laden Sie das Skript herunter.**

   `http://www.sendmail.org/vendor/sun/gen-etc-shells.html`

2. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

3. **Um eine Liste der Shells zu erstellen, führen Sie das Skript `gen-etc-shells` aus.**

   ```
   # ./gen-etc-shells.sh > /tmp/shells
   ```

   Dieses Skript verwendet den Befehl `getent`, um die Namen der Shells zu sammeln, die in den in `/etc/nsswitch.conf` aufgelisteten Passwortdateiquellen enthalten sind.

4. **Prüfen und bearbeiten Sie die Liste der Shells in `/tmp/shells`.**

   Entfernen Sie mithilfe eines von Ihnen gewählten Editors alle Shells, die Sie nicht einbeziehen.

5. **Verschieben Sie die Datei in `/etc/shells`.**

   ```
   # mv /tmp/shells /etc/shells
   ```

Fehlerbehebungsverfahren und Tipps für Mailservices (Übersicht der Schritte)

Die folgende Tabelle enthält Fehlerbehebungsverfahren und Tipps für Mailservices.

Aufgabe	Beschreibung	Siehe
Prüfen der Mailkonfiguration	Schritte zum Prüfen der Änderungen an der `sendmail`-Konfigurationsdatei	„So prüfen Sie die Mailkonfiguration“ auf Seite 343

Aufgabe	Beschreibung	Siehe
Prüfen von Mailaliasen	Ein Schritt, bei dem geprüft wird, ob Mails an einen bestimmten Empfänger übermittelt werden können oder nicht	„So prüfen Sie Mailaliase“ auf Seite 344
Prüfen der Regellisten	Schritte zum Prüfen des Eingangs und der Ausgaben der `sendmail`-Regellisten	„So prüfen Sie die `sendmail`-Regellisten“ auf Seite 345
Verifizieren von Verbindungen mit anderen Systemen	Tipps zum Verifizieren von Verbindungen mit anderen Systemen	„So verifizieren Sie Verbindungen mit anderen Systemen“ auf Seite 346
Protokollieren von Nachrichten mithilfe des `syslogd`-Programms	Tipps zum Sammeln von Informationen zu Fehlermeldungen	„Protokollieren von Fehlermeldungen“ auf Seite 346
Prüfen anderer Quellen auf Diagnoseinformationen	Tipps zum Sammeln von Diagnoseinformationen aus anderen Quellen	„Weitere Quellen für Maildiagnoseinformationen“ auf Seite 347

Fehlerbehebungsverfahren und Tipps für Mailservices

Dieser Abschnitt enthält Verfahren und Tipps, die Sie verwenden können, um Probleme mit Mailservices zu beheben.

▼ So prüfen Sie die Mailkonfiguration

Um die Änderungen zu prüfen, die Sie an Ihrer Konfigurationsdatei vorgenommen haben, befolgen Sie diese Anweisungen.

1 **Starten Sie `sendmail` auf einem System neu, das eine überarbeitete Konfigurationsdatei aufweist.**

```
# svcadm refresh network/smtp:sendmail
```

2 **Senden Sie zu Prüfungszwecken Mails aus jedem System.**

```
# /usr/lib/sendmail -v names </dev/null
```

names Geben Sie die E-Mail-Adresse eines Empfängers an.

Dieser Befehl sendet eine Mail mit dem Wert null an den angegebenen Empfänger und zeigt die Aktivität der Mail auf Ihrem Bildschirm an.

3 **Senden Sie eine Mail an sich selbst oder an andere Personen im lokalen System, indem Sie die Mail an einen normalen Benutzernamen adressieren.**

4 **(Optional) Wenn Ihr System mit einem Netzwerk verbunden ist, senden Sie eine Mail in drei Richtungen an eine Person in einem anderen System:**

- vom Hauptsystem an ein Clientsystem
- von einem Clientsystem an das Hauptsystem
- vom Clientsystem an ein anderes Clientsystem

5 **(Optional) Wenn Sie über ein Mailgateway verfügen, senden Sie eine Mail vom Mailhost an eine andere Domain, um sicherzustellen, dass der Relay Mailer und der Host richtig konfiguriert sind.**

6 **(Optional) Wenn Sie für Ihre Telefonleitung eine UUCP-Verbindung mit einem anderen Host eingerichtet haben, senden Sie über diesen Host eine Mail an eine beliebige Person. Nach dem Empfang der Mail veranlassen Sie die Person, eine Mail zurückzusenden oder Sie zurückzurufen.**

7 **Bitten Sie jemanden, Ihnen über die UUCP-Verbindung eine Mail zuzusenden.**

Das `sendmail`-Programm kann nicht feststellen, ob die Mail gesendet wurde, weil es die Mail, die übermittelt werden soll, an UUCP weitergibt.

8 **Senden Sie von verschiedenen Systemen eine Mail an `postmaster`, und stellen Sie sicher, dass die Mail an die Mailbox Ihres Postmasters übermittelt wird.**

So prüfen Sie Mailaliase

Das folgende Beispiel zeigt, wie Sie ein Alias verifizieren.

```
% mconnect
connecting to host localhost (127.0.0.1), port 25
connection open
220 your.domain.com ESMTP Sendmail 8.13.6+Sun/8.13.6; Tue, 12 Sep 2004 13:34:13 -0800 (PST)
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
221 2.0.0 your.domain.com closing connection
%
```

In diesem Beispiel wurde mithilfe des `mconnect`-Programms eine Verbindung zu einem Mailserver auf einem lokalen Host hergestellt und Ihnen ermöglicht, diese Verbindung zu prüfen. Das Programm ist interaktiv, wodurch Sie verschiedene diagnostische Befehle verwenden können. Eine vollständige Beschreibung finden Sie auf der Manpage `mconnect(1)`. Der Eintrag `expn sandy` stellt die erweiterte Adresse `sandy@phoenix.example.com` bereit. Auf diese Weise können Sie prüfen, ob Mails übermittelt werden können, wenn der Alias `sandy` verwendet wird.

Vermeiden Sie Schleifen und inkonsistente Datenbanken, wenn sowohl lokale als auch domainübergreifende Aliase verwendet werden. Achten Sie insbesondere darauf, die Erstellung von Alias-Schleifen zu vermeiden, wenn Sie einen Benutzer von einem System in ein anderes verschieben.

▼ So prüfen Sie die `sendmail`-Regellisten

Um den Eingang und die Ausgaben der `sendmail`-Regellisten zu prüfen, gehen Sie wie folgt vor.

1 Wechseln Sie in den Adressentestmodus.

```
# /usr/lib/sendmail -bt
```

2 Prüfen Sie eine Mailadresse.

Geben Sie die folgenden Zahlen und die folgende Adresse an der letzten Eingabeaufforderung (>) ein.

> **3,0** *mail-sraddress*

mail-address Verwenden Sie die Mailadresse, die Sie prüfen.

3 Beenden Sie die Sitzung.

Drücken Sie Strg-d.

Beispiel 13–6 Ausgabe des Adressentestmodus

Es folgt ein Beispiel einer Ausgabe des Adressentestmodus.

```
% /usr/lib/sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 sandy@phoenix
canonify           input: sandy @ phoenix
Canonify2          input: sandy < @ phoenix >
Canonify2        returns: sandy < @ phoenix . example . com . >
canonify         returns: sandy < @ phoenix . example . com . >
parse              input: sandy < @ phoenix . example . com . >
Parse0             input: sandy < @ phoenix . example . com . >
Parse0           returns: sandy < @ phoenix . example . com . >
ParseLocal         input: sandy < @ phoenix . example . com . >
ParseLocal       returns: sandy < @ phoenix . example . com . >
Parse1             input: sandy < @ phoenix . example . com . >
MailerToTriple     input: < mailhost . phoenix . example . com >
     sandy < @ phoenix . example . com . >
MailerToTriple   returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
Parse1           returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
parse            returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
```

So verifizieren Sie Verbindungen mit anderen Systemen

Das `mconnect`-Programm stellt eine Verbindung mit einem Mailserver auf einem von Ihnen angegebenen Host her und ermöglicht Ihnen, diese Verbindung zu prüfen. Das Programm ist interaktiv, wodurch Sie verschiedene diagnostische Befehle verwenden können. Eine vollständige Beschreibung finden Sie auf der Manpage `mconnect(1)`. Im folgenden Beispiel wird verifiziert, dass Mails an den Benutzernamen `sandy` übermittelt werden können.

```
% mconnect phoenix

connecting to host phoenix (172.31.255.255), port 25
connection open
220 phoenix.example.com ESMTP Sendmail 8.13.1+Sun/8.13.1; Sat, 4 Sep 2004 3:52:56 -0700
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
```

Wenn es nicht möglich ist, mithilfe von `mconnect` eine Verbindung mit einem `SMTP`-Port herzustellen, prüfen Sie Folgendes:

- Ist die Systembelastung zu hoch?
- Wird der `sendmail`-Dämon ausgeführt?
- Verfügt das System über die entsprechende `/etc/mail/sendmail.cf` -Datei?
- Ist der von `sendmail` verwendete Port 25 aktiv?

Protokollieren von Fehlermeldungen

Ihr Mailservice protokolliert die meisten Fehlermeldungen mithilfe des `syslogd`-Programms. Das `syslogd`-Programm sendet diese Nachrichten standardmäßig an ein System namens `loghost`, das in der `/etc/hosts`-Datei angegeben ist. Sie können `loghost` so definieren, dass alle Protokolle für eine vollständige NSI-Domain enthalten sind. Wenn `loghost` nicht angegeben ist, werden Fehlermeldungen von `syslogd` ausgegeben.

Mit der Datei `/etc/syslog.conf` wird festgelegt, wohin das `syslogd`-Programm die Nachrichten weiterleitet. Sie können die Standardkonfiguration ändern, indem Sie die Datei `/etc/syslog.conf` bearbeiten. Sie müssen den `syslog`-Dämon neu starten, damit Änderungen wirksam werden. Um Informationen über Mails zu sammeln, können Sie Folgendes in die Datei einfügen:

- `mail.alert` – Meldungen über Zustände, die jetzt korrigiert werden sollten
- `mail.crit` – kritische Meldungen
- `mail.warning` – Warnmeldungen
- `mail.notice` – Meldungen, die keine Fehlermeldungen sind, aber beachtet werden sollten

- `mail.info` – informative Meldungen
- `mail.debug` – Fehlersuchmeldungen

Der folgende Eintrag in der Datei `/etc/syslog.conf` sendet eine Kopie aller kritischen, informativen und Fehlersuchmeldungen an `/var/log/syslog`.

```
mail.crit;mail.info;mail.debug              /var/log/syslog
```

Jede Zeile im Systemprotokoll enthält einen Zeitstempel, den Namen des Systems, das die Zeile erstellt hat, und eine Meldung. Die `syslog`-Datei kann eine große Menge von Informationen aufzeichnen.

Das Protokoll besteht aus mehreren Ebenen. Auf der untersten Ebene werden nur ungewöhnliche Ereignisse protokolliert. Auf der höchsten Ebene werden selbst die alltäglichsten und uninteressantesten Ereignisse aufgezeichnet. In der Regel werden Protokollebenen unter 10 als "nützlich" betrachtet. Protokollebenen über 10 werden normalerweise für die Fehlersuche verwendet. Siehe „Customizing System Message Logging“ in *System Administration Guide: Advanced Administration*. In diesem Handbuch finden Sie Informationen über `loghost` und das `syslogd`-Programm.

Weitere Quellen für Maildiagnoseinformationen

Weitere Diagnoseinformationen finden Sie in den folgenden Quellen.

- Achten Sie auf die `Received`-Zeilen in der Kopfzeile der Mail. Diese Zeilen verfolgen den Weg der übermittelten Mail. Berücksichtigen Sie die Zeitzonendifferenzen.
- Achten Sie auf die Meldungen vom `MAILER-DAEMON`. Diese Meldungen weisen typischerweise auf Übermittlungsprobleme hin.
- Prüfen Sie das Systemprotokoll, das Übermittlungsprobleme aufzeichnet, die Ihre Systeme betreffen. Die Aktivitäten des `sendmail`-Programms werden immer im Systemprotokoll aufgezeichnet. Sie können die `crontab`-Datei so modifizieren, dass nachts ein Shell-Skript ausgeführt wird. Das Skript durchsucht das Protokoll nach `SYSERR`-Meldungen und übermittelt gefundene Meldungen an den Postmaster.
- Verwenden Sie das `mailstats`-Programm, um Mailtypen zu prüfen und festzustellen, wie viele Meldungen ein- und ausgehen.

Auflösen von Fehlermeldungen

In diesem Abschnitt wird beschrieben, wie Sie Fehlermeldungen auflösen können, die `sendmail` betreffen. Relevante Informationen finden Sie auch unter `http://www.sendmail.org/faq`.

Die folgenden Fehlermeldungen enthalten zwei oder mehr der folgenden Informationen.

- **Ursache:** Die Ursache für die Ausgabe der Fehlermeldung
- **Beschreibung:** Aktivität des Benutzers zum Zeitpunkt der Ausgabe der Fehlermeldung
- **Lösung:** Was Sie tun können, um das Problem zu beheben oder Ihre Arbeit fortzusetzen

`451 timeout waiting for input during` *source*

Grund: Wenn `sendmail` eine Quelle liest, die eine Zeitüberschreitung auslösen kann (beispielsweise eine SMTP-Verbindung), wird vom Programm ein Timer auf den Wert von verschiedenen Zeitüberschreitungsoptionen gesetzt, bevor der Lesevorgang beginnt. Wenn der Lesevorgang nicht abgeschlossen ist, bevor der Timer abläuft, wird diese Meldung angezeigt und der Lesevorgang stoppt. Diese Situation tritt für gewöhnlich während des `RCPT`-Vorgangs auf. Die Meldung wird dann zur späteren Übermittlung in die Warteschlange gestellt.

Lösung: Wenn diese Meldung häufig angezeigt wird, erhöhen Sie den Wert der verschiedenen Zeitüberschreitungsoptionen in der Datei `/etc/mail/sendmail.cf`. Wenn der Timer bereits auf einen hohen Wert eingestellt ist, suchen Sie nach Hardwareproblemen (beispielsweise schlechte Verkabelungen oder Verbindungen).

`550` *hostname*`... Host unknown`

Grund: Diese `sendmail`-Meldung zeigt an, dass der Zielhost, der hinter dem At-Zeichen (@) der Adresse angegeben ist, nicht während des DNS-Suchvorgangs (Domain Name System) gefunden wurde.

Lösung: Verwenden Sie den Befehl `nslookup`, um zu prüfen, ob der Zielhost in der betreffenden Domain oder in anderen Domains vorhanden ist. Möglicherweise hilft eine leicht veränderte Schreibweise. Wenden Sie sich andernfalls an den Empfänger, um die entsprechende Adresse zu erfragen.

`550` *username*`... User unknown`

Grund: Diese `sendmail`-Meldung zeigt an, dass der Empfänger, der vor dem At-Zeichen (@) der Adresse angegeben ist, nicht auf dem Zielhost gefunden wurde.

Lösung: Überprüfen Sie die E-Mail-Adresse und versuchen Sie es erneut. Möglicherweise hilft eine leicht veränderte Schreibweise. Wenn dies nicht funktioniert, können Sie sich auch an den Empfänger wenden und eine entsprechende Adresse erfragen.

`554` *hostname*`... Local configuration error`

Grund: Diese `sendmail`-Meldung weist in der Regel darauf hin, dass der lokale Host versucht, eine Mail an sich selbst zu senden.

Lösung: Prüfen Sie den Wert des `$j`-Makros in der Datei `/etc/mail/sendmail.cf`, um sicherzustellen, dass dieser Wert ein voll qualifizierter Domainname ist.

Beschreibung: Wenn das sendende System seinen Hostnamen an das empfangende System weitergibt, das im SMTP-`HELO`-Befehl angegeben ist, vergleicht das empfangende System den Namen mit dem Namen des Senders. Wenn diese Namen übereinstimmen, gibt das empfangende System diese Fehlermeldung aus und beendet die Verbindung. Der im `HELO`-Befehl angegebene Name entspricht dem Wert des `$j`-Makros.

Weitere Informationen finden Sie unter `http://www.sendmail.org/faq/section4#4.5`.

`config error: mail loops back to myself.`

Grund: Diese Fehlermeldung wird angezeigt, wenn Sie einen MX-Datensatz erstellen und Host *bar* als Mailübermittler für die Domain *foo* festlegen. Sie können Host *bar* jedoch nicht so konfigurieren, dass dieser erkennt, er ist der Mailübermittler für die Domain *foo* .

Eine andere Möglichkeit besteht darin, dass sowohl das sendende als auch das empfangende System als dieselbe Domain ermittelt werden.

Lösung: Relevante Informationen finden Sie unter `http://www.sendmail.org/faq/section4#4.5`.

`host name configuration error`

Beschreibung: Dies ist eine alte `sendmail`-Meldung, die `I refuse to talk to myself` ersetzte und jetzt durch die Meldung `Local configuration error` ersetzt wurde.

Lösung: Befolgen Sie die Anweisungen zur Auflösung dieser Fehlermeldung `554` *hostname* `... Local configuration error`.

`user unknown`

Grund: Wenn Sie versuchen, eine Nachricht an einen Benutzer zu senden, wird die Fehlermeldung `Username... user unknown` angezeigt. Der Benutzer befindet auf dem gleichen System.

Lösung: Überprüfen Sie die eingegebene E-Mail-Adresse auf Schreibfehler. Andernfalls könnte ein Benutzer-Alias einer nicht vorhandenen E-Mail-Adresse in `/etc/mail/aliases` oder in der Datei `.mailrc` des Benutzers zugeordnet werden. Prüfen Sie zudem, ob im Benutzernamen Großbuchstaben enthalten sind. Bei E-Mail-Adressen ist es von Vorteil, zwischen Groß- und Kleinschreibung nicht zu unterscheiden.

Weitere Informationen finden Sie unter `http://www.sendmail.org/faq/section4#4.17`.

◆ ◆ ◆ KAPITEL 14

Mailservices (Referenz)

Das `sendmail`-Programm ist ein Mail Transport Agent. Das Programm verwendet eine Konfigurationsdatei, um Aliasing, Weiterleitung, automatisches Routing zu Netzwerkgateways und flexible Konfigurationen bereitzustellen. Das Betriebssystem Solaris bietet Standardkonfigurationsdateien, die an den meisten Standorten verwendet werden können. In Kapitel 12, „Mailservices (Übersicht)“ werden die Komponenten der Mailservices vorgestellt. Außerdem wird eine typische Mailservicekonfiguration beschrieben. In Kapitel 13, „Mailservices (Aufgaben)“ wird erläutert, wie ein elektronisches Mailsystem eingerichtet und verwaltet wird. Dieses Kapitel enthält Informationen über folgende Themen:

- „Solaris-Version von `sendmail`“ auf Seite 352
- „Software- und Hardwarekomponenten von Mailservices“ auf Seite 355
- „Mailservice-Programme und -Dateien“ auf Seite 366
- „Mailadressen und Mail-Routing“ auf Seite 386
- „Interaktionen von `sendmail` mit Name Services“ auf Seite 386
- „Änderungen in Version 8.13 von `sendmail`“ auf Seite 392
- „Änderungen ab Version 8.12 von `sendmail`“ auf Seite 400

Einzelheiten, die nicht in diesen Kapiteln behandelt werden, finden Sie auf den folgenden Manpages:

- `sendmail`(1M)
- `mail.local`(1M)
- `mailstats`(1)
- `makemap`(1M)
- `editmap`(1M)

Solaris-Version von sendmail

In diesem Abschnitt, der die folgenden Themen enthält, werden einige der Unterschiede zwischen der Solaris-Version von sendmail und der generischen Berkeley-Version beschrieben.

- „Zum Kompilieren von sendmail verwendete und nicht verwendete Flags“ auf Seite 352
- „MILTER, Mailfilter-API für sendmail“ auf Seite 354
- „Alternative sendmail-Befehle“ auf Seite 354
- „Versionen der Konfigurationsdatei“ auf Seite 354

Zum Kompilieren von sendmail verwendete und nicht verwendete Flags

Ab Solaris 10 werden die folgenden Flags zum Komplieren von sendmail verwendet. Wenn für Ihre Konfiguration andere Flags benötigt werden, müssen Sie die Quelle herunterladen und die Binärversion neu kompilieren. Informationen zu diesem Vorgang finden Sie unter http://www.sendmail.org.

TABELLE 14–1 Allgemeine sendmail-Flags

Flag	Beschreibung
SOLARIS=21000	Unterstützung für Solaris 10
MILTER	Unterstützung für die Mailfilter-API. In Version 8.13 von sendmail ist dieses Flag standardmäßig aktiviert. Lesen Sie dazu „MILTER, Mailfilter-API für sendmail“ auf Seite 354.
NETINET6	Unterstützung für IPv6. Dieses Flag wurde von conf.h nach Makefile verschoben.

TABELLE 14–2 Maps und Datenbanktypen

Flag	Beschreibung
NDBM	Unterstützung für ndbm-Datenbanken
NEWDB	Unterstützung für Berkeley-DB-Datenbanken
USERDB	Unterstützung für die Benutzerdatenbank
NIS	Unterstützung für nis-Datenbanken
NISPLUS	Unterstützung für nisplus-Datenbanken
LDAPMAP	Unterstützung für LDAP-Maps

TABELLE 14–2 Maps und Datenbanktypen *(Fortsetzung)*

Flag	Beschreibung
MAP_REGEX	Unterstützung für Maps für reguläre Ausdrücke

TABELLE 14–3 Betriebssystem-Flags

Flag	Beschreibung
SUN_EXTENSIONS	Unterstützung für Sun-Erweiterungen, die in _compat.o enthalten sind
SUN_INIT_DOMAIN	Für die Abwärtskompatibilität werden NIS-Domainnamen unterstützt, damit der Name des lokalen Hosts vollständig qualifiziert werden kann. Weitere anbieterspezifische Informationen finden Sie unter http://www.sendmail.org.
SUN_SIMPLIFIED_LDAP	Unterstützung für eine vereinfachte LDAP-API, die speziell für Sun ausgelegt ist. Weitere anbieterspezifische Informationen finden Sie unter http://www.sendmail.org.
VENDOR_DEFAULT=VENDOR_SUN	Wählt Sun als Standardanbieter aus.

In der folgenden Tabelle werden generische Flags aufgelistet, die nicht verwendet werden, um die Version von sendmail zu kompilieren, die mit Solaris 10 mitgeliefert wird.

TABELLE 14–4 Nicht in dieser Version von sendmail verwendete generische Flags

Flag	Beschreibung
SASL	Simple Authentication and Security Layer (RFC 2554)
STARTTLS	Transaction Level Security (RFC 2487)

Um eine Liste der Flags anzuzeigen, die zum Kompilieren von sendmail dienen, verwenden Sie den folgenden Befehl.

```
% /usr/lib/sendmail -bt -d0.10 < /dev/null
```

Hinweis – Der vorhergehende Befehl listet nicht die für Sun spezifischen Flags auf.

MILTER, Mailfilter-API für sendmail

MILTER, die Mailfilter-API von sendmail, ermöglicht Programmen von Drittanbietern, auf Mails zuzugreifen, während diese verarbeitet werden. Dadurch können Metadaten und Inhalte gefiltert werden. Es ist nicht nötig, den Filter zu erstellen und sendmail zu konfigurieren, um diese API zu verwenden. Diese API ist in Version 8.13 von sendmail standardmäßig aktiviert.

Weitere Informationen finden Sie hier:

- http://www.sendmail.org
- https://www.milter.org/

Alternative sendmail-Befehle

Die Solaris-Version enthält nicht alle Befehlssynonyme, die in der generischen Version von sendmail.org enthalten sind. Diese Tabelle enthält eine vollständige Liste der Befehlsaliase. In der Tabelle wird auch angegeben, ob die Befehle in der Solaris-Version enthalten sind und wie dasselbe Verhalten mithilfe von sendmail hervorgerufen wird.

TABELLE 14–5 Alternative sendmail-Befehle

Name des alternativen Befehls	In dieser Version enthalten?	Optionen mit sendmail
hoststat	Nein	sendmail -bh
mailq	Ja	sendmail -bp
newaliases	Ja	sendmail -bi
purgestat	Nein	sendmail -bH
smtpd	Nein	sendmail -bd

Versionen der Konfigurationsdatei

Ab Solaris 10 enthält sendmail eine Konfigurationsoption, die Ihnen ermöglicht, die Version der Datei sendmail.cf zu definieren. Diese Option gestattet, ältere Konfigurationsdateien zusammen mit der aktuellen Version von sendmail zu verwenden. Sie können den Versionsstand auf Werte zwischen 0 und 10 setzen. Sie können zudem den Anbieter definieren. Eine gültige Anbieteroption ist entweder Berkeley oder Sun. Wenn ein Versionsstand, aber kein Anbieter angegeben ist, wird Sun als standardmäßiger Anbieter verwendet. In der folgenden Tabelle werden einige der gültigen Optionen aufgelistet.

TABELLE 14–6 Versionswerte für die Konfigurationsdatei

Bereich	Beschreibung
`V7/Sun`	Diese Einstellung wurde für Version 8.8 von `sendmail` verwendet.
`V8/Sun`	Diese Einstellung wurde für Version 8.9 von `sendmail` verwendet. Diese Einstellung wurde in Solaris 8 aufgenommen.
`V9/Sun`	Diese Einstellung wurde für die Versionen 8.10 und 8.11 von `sendmail` verwendet.
`V10/Sun`	Diese Einstellung wurde für die Versionen 8.12 und 8.13 von `sendmail` verwendet. Version 8.12 ist die Standardversion für Solaris 9. Ab Solaris 10 ist Version 8.13 die Standardversion.

Hinweis – Es wird nachdrücklich empfohlen, `V1/Sun` nicht zu verwenden. Weitere Informationen finden Sie unter `http://www.sendmail.org/vendor/sun/differences.html#4`.

Aufgabenbezogene Informationen finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“.

Software- und Hardwarekomponenten von Mailservices

In diesem Abschnitt werden die Software- und Hardwarekomponenten eines Mailsystems beschrieben.

- „Softwarekomponenten“ auf Seite 355
- „Hardwarekomponenten“ auf Seite 363

Softwarekomponenten

Jeder Mailservice enthält mindestens eine der folgenden Softwarekomponenten:

- „Mail-Benutzeragent“ auf Seite 356
- „Mail Transfer Agent“ auf Seite 356
- „Lokaler Delivery Agent“ auf Seite 356

In diesem Abschnitt werden auch die folgenden Softwarekomponenten beschrieben:

- „Mailer und `sendmail`“ auf Seite 356
- „Mailadressen“ auf Seite 358
- „Mailbox-Dateien“ auf Seite 360
- „Mailaliase“ auf Seite 362

Mail-Benutzeragent

Der *Mail-Benutzeragent* ist ein Programm, das als Schnittstelle zwischen dem Benutzer und dem Mail Transfer Agent fungiert. Das `sendmail`-Programm ist ein Mail Transfer Agent. Das Betriebssystem Solaris stellt die folgenden Mailbenutzeragenten bereit:

- `/usr/bin/mail`
- `/usr/bin/mailx`
- `/usr/dt/bin/dtmail`

Mail Transfer Agent

Der *Mail Transfer Agent* ist für die Weiterleitung von Mails und die Auflösung von Mailadressen verantwortlich. Dieser Agent wird auch als Mail *Transport* Agent bezeichnet. Der Transfer Agent für das Betriebssystem Solaris ist `sendmail`. Der Transfer Agent führt folgende Funktionen aus:

- Nimmt Nachrichten vom Mail-Benutzeragenten an
- Löst Zieladressen auf
- Wählt einen entsprechenden Delivery Agent für die Übermittlung der Mail aus
- Empfängt eingehende Mails von anderen Mail Transfer Agents

Lokaler Delivery Agent

Ein *lokaler Delivery Agent* ist ein Programm, das ein Mail-Übermittlungsprotokoll implementiert. Folgende lokale Delivery Agents werden im Betriebssystem Solaris bereitgestellt:

- Der lokale UUCP Delivery Agent, der `uux` verwendet, um Mails zu übermitteln
- Der lokale Delivery Agent, der `mail.local` in der standardmäßigen Solaris-Version enthalten ist

Weitere Informationen zu diesen Themen finden Sie unter „Änderungen ab Version 8.12 von `sendmail`“ auf Seite 400.

- „Zusätzliche Delivery Agents-Flags ab Version 8.12 von `sendmail`“ auf Seite 412
- „Zusätzliche Gleichsetzungen für Delivery Agents ab Version 8.12 von `sendmail`“ auf Seite 412

Mailer und `sendmail`

Mailer ist ein `sendmail`-spezifischer Begriff. Ein *Mailer* wird von `sendmail` verwendet, um eine bestimmte Instanz eines angepassten lokalen Delivery Agent oder eines angepassten Mail Transfer Agent zu bestimmen. Sie müssen mindestens einen Mailer in Ihrer `sendmail.cf` -Datei angeben. Aufgabenbezogene Informationen finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“. Dieser Abschnitt enthält eine kurze Beschreibung der beiden Mailertypen.

- „SMTP-Mailer (Simple Mail Transfer Protocol)“ auf Seite 357
- „UUCP-Mailer (UNIX-to-UNIX Copy Program)“ auf Seite 357

Weitere Informationen zu Mailern finden Sie unter `http://www.sendmail.org/m4/readme.html` oder in der Datei `/etc/mail/cf/README`.

SMTP-Mailer (Simple Mail Transfer Protocol)

SMTP ist das standardmäßige Mailprotokoll, das im Internet verwendet wird. Dieses Protokoll definiert diese Mailer.

- `smtp` sorgt für die normale SMTP-Übertragung an andere Server.
- `esmtp` sorgt für die erweiterte SMTP-Übertragung an andere Server.
- `smtp8` sorgt für die SMTP-Übertragung an andere Server, ohne 8-Bit-Daten in MIME zu konvertieren.
- `dsmtp` sorgt für eine bedarfsorientierte Übermittlung mithilfe des Mailer-Flags `F=%`. Lesen Sie dazu „Änderungen an der `MAILER()`-Deklaration ab Version 8.12 von `sendmail`“ auf Seite 411 und „Zusätzliche Delivery Agents-Flags ab Version 8.12 von `sendmail`“ auf Seite 412.

UUCP-Mailer (UNIX-to-UNIX Copy Program)

Die Verwendung von UUCP ist nach Möglichkeit zu vermeiden. Eine Erläuterung finden Sie unter `http://www.sendmail.org/m4/uucp_mailers.html`. Auch können Sie die Datei `/etc/mail/cf/README` durchsuchen, indem Sie diese Zeichenfolge verwenden: `USING UUCP MAILERS`.

UUCP definiert diese Mailer.

`uucp-old` Namen in der `$=U`-Klasse werden an `uucp-old` gesendet. `uucp` ist der veraltete Name für diesen Mailer. Der `uucp-old` Mailer verwendet in diesen Kopfzeilen eine Adresse mit Ausrufezeichen.

`uucp-new` Namen in der `$=Y`-Klasse werden an `uucp-new` gesendet. Verwenden Sie diese Mailer, wenn Sie wissen, dass der empfangende UUCP-Mailer mehrere Empfänger in einer Übertragung verwalten kann. `suucp` ist der veraltete Name für diesen Mailer. Der `uucp-new`-Mailer verwendet ebenfalls in diesen Kopfzeilen eine Adresse mit Ausrufezeichen.

Wenn `MAILER(smtp)` ebenfalls in Ihrer Konfiguration angegeben ist, sind zwei weitere Mailer definiert.

`uucp-dom` Dieser Mailer verwendet Domain-basierte Adressen und wendet in der Regel die SMTP-Umschreibungsregeln an.

`uucp-uudom` Namen in der `$=Z`-Klasse werden an `uucp-uudom` gesendet. `uucp-uudom` und `uucp-dom` verwenden dieselben Domain-basierte Adressen mit Kopfzeilen-Adressformat.

Hinweis – Da der `smtp`-Mailer den UUCP-Mailer modifiziert, fügen Sie `MAILER(smtp)` stets vor `MAILER(uucp)` in Ihre `.mc`-Datei ein.

Mailadressen

Die *Mailadresse* enthält den Namen des Empfängers und des Systems, an das die Mail übermittelt wird. Wenn Sie ein kleines Mailsystem verwalten, das keinen Name Service verwendet, ist die Adressierung von Mails ein leichtes Unterfangen. Die Anmeldenamen kennzeichnen eindeutig die Benutzer. Komplexität entsteht, wenn Sie ein Mailsystem verwalten, das mehrere Mailboxsysteme oder mehrere Domains aufweist. Des Weiteren kann Komplexität entstehen, wenn Sie eine UUCP-Mailverbindung (oder eine andere Verbindung) mit Servern außerhalb Ihres Netzwerks verwenden. Die in den folgenden Abschnitten enthaltenen Informationen können Ihnen helfen, die Teile und die Komplexität von Mailadressen besser zu verstehen.

- „Domains und Teildomains“ auf Seite 358
- „Name der Name Service-Domain und Name der Maildomain“ auf Seite 359
- „Typisches Format für Mailadressen“ auf Seite 359
- „Routenunabhängige Mailadressen“ auf Seite 360

Domains und Teildomains

Für die Adressierung von E-Mails werden Domains verwendet. Eine *Domain* ist eine Verzeichnisstruktur für das Netzwerkadressen-Naming. Eine Domain kann eine oder mehrere *Teildomains* haben. Die Domain und die Teildomains einer Adresse können mit der Hierarchie eines Dateisystems verglichen werden. Es wird vorausgesetzt, dass nur ein Unterverzeichnis im übergeordneten Verzeichnis enthalten ist. In gleicher Weise wird vorausgesetzt, dass jede Teildomain im rechten Teil einer Mailadresse enthalten ist.

Die folgende Tabelle zeigt einige Domains der obersten Ebene.

TABELLE 14–7 Domains der obersten Ebene

Domain	Beschreibung
`com`	Kommerzielle Websites
`edu`	Bildungs-Websites
`gov`	Installationen der US-Regierung

TABELLE 14–7 Domains der obersten Ebene *(Fortsetzung)*

Domain	Beschreibung
`mil`	Installationen des US-Militärs
`net`	Vernetzte Organisationen
`org`	Weitere Non-Profit-Organisationen

Für Domains gilt die Unterscheidung zwischen Groß- und Kleinschreibung. Im Teil der Adresse, der für die Domain bestimmt ist, können Sie Großbuchstaben, Kleinbuchstaben oder beides verwenden, ohne dass dadurch Fehler entstehen.

Name der Name Service-Domain und Name der Maildomain

Wenn Sie mit Namen von Name Service-Domains und Namen von Maildomains arbeiten, ist Folgendes zu beachten:

- Das `sendmail`-Programm entfernt standardmäßig die erste Komponente des NIS- oder NIS+-Domainnamens, um den Namen der Maildomain zu bilden. Wenn eine NIS+-Domain beispielsweise `bldg5.example.com` wäre, würde der Name der entsprechenden Maildomain `example.com` lauten.
- Obwohl bei Maildomainadressen zwischen Groß- und Kleinschreibung unterschieden wird, ist dies bei NIS- oder NIS+-Domainnamen nicht der Fall. Um beste Ergebnisse zu erzielen, empfiehlt es sich, beim Anlegen der Mail- und NIS- oder NIS+-Domainnamen Kleinbuchstaben zu verwenden.
- Der DNS-Domainname und der Name der Maildomain müssen identisch sein.

Weitere Informationen finden Sie unter „Interaktionen von `sendmail` mit Name Services“ auf Seite 386.

Typisches Format für Mailadressen

Eine Mailadresse hat das folgende Format. Weitere Informationen finden Sie unter „Routenunabhängige Mailadressen“ auf Seite 360.

user@subdomain. subdomain2.subdomain1.top-level-domain

Der links neben dem `@`-Zeichen stehende Teil der Adresse ist die lokale Adresse. Die lokale Adresse kann Folgendes enthalten:

- Informationen zum Routing mit einem anderen Mail-Übermittlungssystem (beispielsweise `bob::vmsvax@gateway` oder `smallberries%mill.uucp@gateway`)
- Ein Alias (beispielsweise `iggy.ignatz`)

Hinweis – Der empfangende Mailer muss bestimmen, was der lokale Teil der Adresse bedeutet. Informationen zu Mailern finden Sie unter „Mailer und `sendmail`“ auf Seite 356.

Der rechts neben dem `@`-Zeichen stehende Teil der Adresse zeigt die Domainebenen, in denen sich die lokale Adresse befindet. Jede Teildomain wird durch einen Punkt getrennt. Der Domainteil der Adresse kann eine Organisation, ein physischer Bereich oder eine geografische Region sein. Außerdem ist die Reihenfolge der Domaininformationen hierarchisch, d. h., je lokaler die Teildomain, desto näher steht die Teildomain zum `@`-Zeichen.

Routenunabhängige Mailadressen

Mailadressen können unabhängig weitergeleitet werden. Die routenunabhängige Adressierung erfordert, dass der Absender einer E-Mail-Nachricht den Namen des Empfängers und das endgültige Ziel angibt. Ein Hochgeschwindigkeitsnetzwerk wie das Internet verwendet routenunabhängige Adressen. Routenunabhängige Adressen können folgendes Format haben:

user`@`*host*`.`*domain*

Routenunabhängige Adressen für UUCP-Verbindungen können folgendes Format haben:

host`.`*domain*`!`*user*

Dank zunehmender Popularität von Domain-basierten hierarchischen Naming-Schemata für Computer finden routenunabhängige Adressen verbreitet Verwendung. In der am häufigsten verwendeten routenunabhängigen Adresse wird der Hostname weggelassen und darauf vertraut, dass der Name Service der Domain das endgültige Ziel der E-Mail-Nachricht bestimmt.

user`@`*domain*

Routenunabhängige Adressen werden gelesen, indem zunächst nach dem `@`-Zeichen gesucht wird. Die Domainhierarchie wird dann von rechts (der höchsten Ebene) nach links (dem rechts neben dem `@`-Zeichen stehenden spezifischsten Teil der Adresse) gelesen.

Mailbox-Dateien

Bei einer *Mailbox* handelt es sich um eine Datei, die das endgültige Ziel für E-Mail-Nachrichten ist. Der Name der Mailbox kann ein Benutzername oder die Identität einer speziellen Funktion sein, wie beispielsweise Postmaster. Mailboxen befinden sich in der `/var/mail/`*username*-Datei, die sich entweder auf dem lokalen System des Benutzers oder auf einem Remote-Mailserver befinden kann. In beiden Fällen befindet sich die Mailbox auf dem System, an das die Mail übermittelt wird.

Mails sollten immer an ein lokales Dateisystem übermittelt werden, damit der Benutzeragent Mails aus dem Mail-Spool-Verzeichnis entnehmen und in der lokalen Mailbox speichern kann. Verwenden Sie keine über NFS eingehängten Dateisysteme als Ziel für die Mailbox eines

Benutzers. Insbesondere sollten Sie keine Mails an einen Mailclient weiterleiten, der das `/var/mail`-Dateisystem von einem Remote-Server einhängt. Mails für den Benutzer sollten in diesem Fall an den Mailserver und nicht an den Clienthost adressiert sein. Über NFS eingehängte Dateisysteme können Probleme mit der Übermittlung und Verarbeitung von Mails verursachen.

Die `/etc/mail/aliases`-Datei und Name Services wie NIS und NIS+ stellen Mechanismen bereit, die es ermöglichen, Aliase für elektronische Mailadressen zu erstellen. Aus diesem Grunde müssen Benutzer nicht den genauen lokalen Namen der Mailbox eines Benutzers kennen.

In der nachstehenden Tabelle sind einige allgemeine Naming-Konventionen für spezielle Mailboxen aufgeführt.

TABELLE 14–8 Konventionen für das Format von Mailbox-Namen

Format	Beschreibung
username	Benutzernamen stimmen häufig mit Mailbox-Namen überein.
Firstname`.` *Lastname* *Firstname*`_` *Lastname* *Firstinitial*`.` *Lastname* *Firstinitial*`_` *Lastname*	Benutzernamen können als vollständige Namen mit einem Punkt (oder einem Unterstrich) identifiziert werden, der den Vornamen und den Nachnamen trennt. Auch können Benutzernamen durch einen Anfangsbuchstaben mit einem Punkt (oder einem Unterstrich) gekennzeichnet werden, der zwischen dem Anfangsbuchstaben und Nachnamen steht.
`Postmaster`	Mit dem Mailsystem der `Postmaster`-Mailbox können Benutzer Fragen stellen und Probleme melden. Jeder Standort und jede Domain sollten eine `Postmaster`-Mailbox haben.
`MAILER-DAEMON`	`sendmail` leitet automatisch Mails weiter, die über `MAILER-DAEMON` an den Postmaster adressiert sind.
aliasname`-request`	Namen, die auf `-request` enden, sind administrative Adressen für Verteilungslisten. Diese Adresse leitet Mails an die Person weiter, die die Verteilungsliste verwaltet.
`owner-`*aliasname*	Namen, die mit `owner-` beginnen, sind administrative Adressen für Verteilungslisten. Diese Adresse leitet Mails an die Person weiter, die sich um Mail-Übermittlungsfehler kümmert.
`owner-owner`	Dieser Alias wird verwendet, wenn kein `owner-`*aliasname*-Alias vorhanden ist, an den Fehler zurückgegeben werden können. Diese Adresse leitet Mails an die Person weiter, die sich um Mail-Übermittlungsfehler kümmert. Diese Adresse sollte auf einem System definiert sein, dass eine große Anzahl von Aliasen verwaltet.
local`%`*domain*	Das Prozentzeichen (`%`) bezeichnet eine lokale Adresse, die erweitert wird, wenn die Mail am Ziel ankommt. Die meisten Mailsysteme interpretieren Mailbox-Namen mit `%`-Zeichen als vollständige Mailadressen. Das `%`-Zeichen wird durch ein `@`-Zeichen ersetzt und die Mail dementsprechend weitergeleitet. Obwohl viele Benutzer die `%`-Konvention verwenden, ist diese Konvention kein formaler Standard. Diese Konvention wird als "Prozent-Hack" bezeichnet. Diese Funktion wird oft verwendet, um Mailprobleme zu beheben.

Ab `sendmail`-Version 8 wird der Absender der Mails, die an ein Gruppenalias gesendet werden, in die Adresse geändert, die aus dem Eigentümeralias erweitert wurde, sofern ein Eigentümeralias vorhanden ist. Durch diese Änderung können Mailfehler an den

Aliaseigentümer gesendet werden und müssen nicht an den Absender zurückgegeben werden. Auch werden Benutzer bemerken, dass die an einen Alias gesendeten Mails scheinbar vom Aliasaigentümer kommen, wenn sie übermittelt werden. Das folgende Aliasformat hilft bei der Behebung von Problemen, die mit dieser Änderung verbunden sind.

```
mygroup: :include:/pathname/mygroup.list
owner-mygroup: mygroup-request
mygroup-request: sandys, ignatz
```

In diesem Beispiel ist das Alias `mygroup` das aktuelle Mailalias für die Gruppe. Das Alias `owner-mygroup` empfängt Fehlermeldungen. Das Alias `mygroup-request` sollte für administrative Anfragen verwendet werden. Das bedeutet, dass in Mails, die an das Alias `mygroup` gesendet werden, der Absender in `mygroup-request` geändert wird.

Mailaliase

Ein *Alias* ist ein alternativer Name. Für E-Mails können Sie Aliase verwenden, um eine Mailbox-Adresse zuzuweisen oder Mailing-Listen zu definieren. Eine Übersicht der Schritte finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“. Weitere Informationen finden Sie in diesem Kapitel auch unter „Mail-Aliasdateien“ auf Seite 379.

Bei großen Standorten definiert der Mailalias in der Regel die Adresse einer Mailbox. Die Bereitstellung eines Mailalias ist vergleichbar mit der Angabe einer Zimmernummer als Teil der Adresse einer Person, die in einem großen Unternehmen beschäftigt ist. Um bei diesem Beispiel zu bleiben: Wenn Sie keine Zimmernummer angeben, wird die Mail an eine zentrale Stelle übermittelt. Ohne Zimmernummer ist zusätzlicher Aufwand nötig, um herauszufinden, wohin im Gebäude die Mail übermittelt werden kann. Dementsprechend ist die Wahrscheinlichkeit größer, dass ein Fehler auftritt. Wenn sich beispielsweise zwei Personen mit demselben Namen im selben Gebäude befinden, kann die Mail eventuell nur an eine dieser Personen übermittelt werden. Um dieses Problem zu vermeiden, muss nur die jeweilige Zimmernummer angegeben werden.

Verwenden Sie möglichst Adressen, die von Domains und Standorten unabhängig sind, wenn Sie Mailing-Listen erstellen. Um die Übertragbarkeit und Flexibilität von Aliasdateien zu verbessern, sollten Ihre Aliaseinträge in den Mailing-Listen so generisch und systemunabhängig wie möglich sein. Wenn beispielsweise ein Benutzer namens `ignatz` im System `mars` in der Domain `example.com` vorhanden ist, erstellen Sie den Alias `ignatz@example` anstelle von `ignatz@mars`. Wenn der Benutzer `ignatz` den Namen seines Systems ändert, aber weiterhin in der Domain `example` zu finden ist, müssen Sie keine Aliasdateien aktualisieren, um die Änderung des Systemnamens zu reflektieren.

Wenn Sie Aliaseinträge erstellen, tragen Sie jeweils ein Alias pro Zeile ein. Es sollte nur ein Eintrag vorhanden sein, der den Systemnamen des Benutzers enthält. Beispielsweise können Sie folgende Einträge für den Benutzer `ignatz` erstellen:

```
ignatz: iggy.ignatz
iggyi: iggy.ignatz
iggy.ignatz: ignatz@mars
```

Sie können ein Alias für lokale Namen oder Domains erstellen. Beispielsweise kann ein Aliaseintrag für den Benutzer `fred`, der eine Mailbox im System `mars` hat und in der Domain `planets` zu finden ist, einen solchen Eintrag in der NIS+-Aliastabelle aufweisen.

```
fred: fred@planets
```

Wenn Sie Mailing-Listen erstellen, in denen Benutzer außerhalb Ihrer Domain enthalten sind, erstellen Sie den Alias mit dem Benutzernamen und dem Domainnamen. Wenn beispielsweise ein Benutzer namens `smallberries` im System `privet` in der Domain `example.com` vorhanden ist, erstellen Sie den Alias in der Form von `smallberries@example.com`. Die E-Mail-Adresse des Absenders wird nun automatisch in einen voll qualifizierten Domainnamen umgewandelt, wenn Mails die Domain des Benutzers verlassen.

In der folgenden Liste sind Verfahren zum Erstellen und Verwalten von Mailaliasdateien beschrieben.

- Sie können Mailaliase zur globalen Verwendung in der NIS+-Tabelle `mail_aliases`, in der NIS-Map `aliases` oder in lokalen `/etc/mail/aliases`-Dateien erstellen. Auch können Sie Mailing-Listen erstellen und verwalten, die dieselben Aliasdateien verwenden.
- Je nach der Konfiguration Ihrer Mailservices können Sie mithilfe des NIS- oder NIS+-Name Service Aliase zuweisen, um eine globale `Alias`-Datenbank zu verwalten. Sie haben aber auch die Möglichkeit, alle lokalen `/etc/mail/aliases`-Dateien zu aktualisieren, um für die Übereinstimmung der Aliase zu sorgen.
- Benutzer können ebenfalls Aliase erstellen und verwenden. Benutzer können Aliase entweder in ihrer lokalen `~/.mailrc`-Datei erstellen, die nur von den jeweiligen Benutzern selbst verwendet werden kann, oder in der lokalen `/etc/mail/aliases`-Datei, die von allen Benutzern verwendet werden kann. Benutzer können normalerweise keine NIS- oder NIS+-Aliasdateien erstellen oder verwalten.

Hardwarekomponenten

Sie können die drei erforderlichen Elemente der Mailkonfiguration im selben oder verschiedenen Systemen bereitstellen.

- „Mailhost“ auf Seite 364
- „Mailserver“ auf Seite 364
- „Mailclient“ auf Seite 365

Wenn Benutzer mit Netzwerken außerhalb Ihrer Domain kommunizieren sollen, müssen Sie ein viertes Element – ein Mailgateway – hinzufügen. Weitere Informationen finden Sie unter „Mailgateway“ auf Seite 365. In den folgenden Abschnitten werden die einzelnen Hardwarekomponenten beschrieben.

Mailhost

Ein *Mailhost* ist ein Rechner, den Sie als Hauptmailrechner in Ihrem Netzwerk festlegen. Ein Mailhost ist ein Rechner, an das anderen Systeme des Standorts Mails weiterleiten, die nicht übermittelt werden können. Sie legen ein System als Mailhost in der `hosts`-Datenbank fest, indem Sie das Wort `mailhost` rechts neben der IP-Adresse in der lokalen `/etc/hosts`-Datei angeben. Auch können Sie das Wort `mailhost` in gleicher Weise in der Hostdatei im Name Service angeben. Ausführliche aufgabenbezogene Informationen finden Sie unter „So richten Sie einen Mailhost ein“ auf Seite 309 in Kapitel 13, „Mailservices (Aufgaben)“.

Ebenfalls eignet sich ein System als Mailhost, das in Ihrem System als Router für das Internet konfiguriert ist. Weitere Informationen finden Sie in Kapitel 15, „Solaris PPP 4.0 (Überblick)“, Kapitel 24, „UUCP (Übersicht)“ und unter „Konfiguration eines IPv4-Routers“ in *Systemverwaltungshandbuch: IP Services*. Wenn kein System in Ihrem lokalen Netzwerk ein Modem hat, legen Sie ein System als Mailhost fest.

An manchen Standorten werden eigenständige Rechner verwendet, die nicht in einer Timesharing-Konfiguration vernetzt sind. Der eigenständige Rechner übermittelt Daten an Terminals, die an seine seriellen Ports angeschlossen sind. Sie können die elektronische Übermittlung von Mails für die Konfiguration einrichten, indem Sie das eigenständige System als Mailhost eines eigenständigen Netzwerks festlegen. Im Abschnitt „Übersicht der Hardwarekomponenten“ auf Seite 296 in Kapitel 12, „Mailservices (Übersicht)“ finden Sie ein Abbildung, die eine typische E-Mail-Konfiguration zeigt.

Mailserver

Eine *Mailbox* ist eine einzelne Datei, die E-Mails für einen bestimmten Benutzer enthält. Die Mails werden an das System übermittelt, in dem sich die Mailbox des Benutzers befindet. Dies kann ein lokaler Rechner oder ein Remote-Server sein. Ein *Mailserver* ist ein System, das Benutzer-Mailboxen in seinem Verzeichnis `/var/mail` verwaltet. Aufgabenbezogene Informationen finden Sie unter „Einrichten eines Mailservers“ auf Seite 305 in Kapitel 13, „Mailservices (Aufgaben)“.

Der Mailserver leitet alle Mails weiter, die von einem Client kommen. Wenn ein Client eine Mail sendet, stellt der Mailserver die Mail zur späteren Übermittlung in eine Warteschlange. Nachdem die Mail in die Warteschlange gestellt wurde, kann ein Benutzer den Client neu booten oder ausschalten, ohne dass diese Mails verloren gehen. Wenn der Empfänger eine Mail von einem Client erhält, enthält der Pfad in der Zeile `Von` der Mail den Namen des Mailservers. Wenn der Empfänger antwortet, wird die Antwort an die Mailbox des Benutzers gesendet. Als Mailserver eignen sich Systeme, die ein Home-Verzeichnis für Benutzer oder Systeme bieten, die regelmäßig gesichert werden.

Wenn der Mailserver nicht das lokale System des Benutzers ist, können Benutzer in Konfigurationen, die NFS-Software verwenden, das `/var/mail`-Verzeichnis einhängen, indem sie die `/etc/vfstab`-Datei verwenden, sofern sie `root`-Zugriff haben. Anderenfalls können die Benutzer den Automounter verwenden. Wenn NFS nicht unterstützt wird, können sich die Benutzer beim Server anmelden, um ihre Mails zu lesen.

Wenn die Benutzer in Ihrem Netzwerk andere Mailtypen wie beispielsweise Audiodateien oder Dateien von Desktop-Publishing-Systemen versenden, müssen Sie mehr Speicherplatz auf dem Mailserver für die Mailboxen bereitstellen.

Durch die Festlegung eines Mailservers für alle Mailboxen können Sie den Sicherungsprozess vereinfachen. Sicherungen können sich schwierig gestalten, wenn Mails auf viele Systeme verteilt werden. Der Nachteil von vielen Mailboxen auf einem Server ist der, dass der Server für viele Benutzer eine Schwachstelle sein kann. Jedoch wiegen die Vorteile von guten Sicherungen dieses Risiko in der Regel auf.

Mailclient

Ein Mailclient ist ein Benutzer eines Mailservice mit einer Mailbox auf einem Mailserver. Außerdem hat ein Mailclient einen Mailalias in der `/etc/mail/aliases`-Datei, die auf die Adresse der Mailbox verweist. Aufgabenbezogene Informationen finden Sie unter „So richten Sie einen Mailclient ein“ auf Seite 307 in Kapitel 13, „Mailservices (Aufgaben)“.

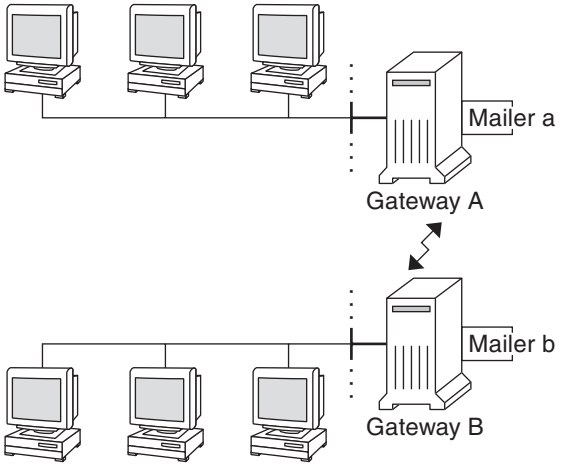
Mailgateway

Das *Mailgateway* ist ein Rechner, der Verbindungen zwischen Netzwerken koordiniert, in denen verschiedene Kommunikationsprotokolle oder Kommunikationssysteme verwendet werden, die zur Kommunikation zwischen verschiedenen Netzwerken dienen, die dasselbe Protokoll verwenden. Ein Mailgateway kann beispielsweise ein TCP/IP-Netzwerk mit einem Netzwerk verbinden, in dem die SNA-Protokollfamilie (Systems Network Architecture) ausgeführt wird.

Das einfachste Mailgateway, das eingerichtet werden kann, ist ein Mailgateway, das zwei Netzwerke verbindet, die dasselbe Protokoll oder denselben Mailer verwenden. Dieses System sorgt für die Übermittlung von Mails mit einer Adresse, für die `sendmail` keinen Empfänger in Ihrer Domain finden kann. Wenn ein Mailgateway vorhanden ist, verwendet `sendmail` das Gateway, um Mails aus Ihrer Domain herauszusenden und Mails in Ihrer Domain zu empfangen, die von außerhalb kommen.

Sie können ein Mailgateway zwischen zwei Netzwerken einrichten, die ungleiche Mailer verwenden (siehe nachstehende Abbildung). Um diese Konfiguration zu unterstützen, müssen Sie die Datei `sendmail.cf` im Mailgatewaysystem anpassen, was schwierig und zeitaufwändig sein kann.

ABBILDUNG 14–1 Gateway zwischen verschiedenen Kommunikationsprotokollen



Wenn Sie einen Rechner verwenden, der Verbindungen mit dem Internet herstellt, können Sie diesen Rechner als Mailgateway konfigurieren. Wägen Sie sorgfältig die Sicherheitsanforderungen Ihres Standorts ab, bevor Sie ein Mailgateway konfigurieren. Unter Umständen müssen Sie ein Firewall-Gateway zwischen Ihrem Firmennetzwerk und anderen Netzwerken einrichten und dieses Gateway dann als Mailgateway definieren. Aufgabenbezogene Informationen finden Sie unter „So richten Sie ein Mailgateway ein“ auf Seite 310 in Kapitel 13, „Mailservices (Aufgaben)“.

Mailservice-Programme und -Dateien

Mailservices enthalten viele Programme und Dämonen, die miteinandern interagieren. In diesem Abschnitt werden Dateien, Programme, Begriffe und Konzepte vorgestellt, die im Zusammenhang mit der Verwaltung von elektronisch übermittelten Mails stehen.

- „Verbesserung des Dienstprogramms `vacation`“ auf Seite 367
- „Inhalt des `/usr/bin`-Verzeichnisses“ auf Seite 367
- „Inhalt des `/etc/mail`-Verzeichnisses“ auf Seite 368
- „Inhalt des `/usr/lib`-Verzeichnisses“ auf Seite 372
- „Weitere Dateien, die für Mailservices verwendet werden“ auf Seite 372
- „Interaktionen von Mailprogrammen“ auf Seite 374
- „`sendmail`-Programm“ auf Seite 375
- „Mail-Aliasdateien“ auf Seite 379
- „`.forward`-Dateien“ auf Seite 382
- „`/etc/default/sendmail`-Datei“ auf Seite 384

Verbesserung des Dienstprogramms `vacation`

Ab Solaris 10 wurde das Dienstprogramm `vacation` verbessert. Der Benutzer kann nun festlegen, welche eingehenden Mails eine automatisch generierte Antwort erhalten sollen. Dadurch kann eine Weitergabe von vertraulichen Informationen oder Kontaktangaben an Unbekannte verhindert werden. Nachrichten von Spam-Absendern oder unbekannten Personen erhalten auf diese Weise keine Antwort.

Die Funktionsweise dieser Verbesserung besteht darin, dass die E-Mail-Adresse einer eingehenden E-Mail des Absenders mit einer Liste von Domains oder E-Mail-Adressen in einer `.vacation.filter`-Datei verglichen wird. Diese Datei wird vom Benutzer erstellt und befindet sich im Home-Verzeichnis des Benutzers. Wenn in der Liste eine Übereinstimmung mit der Domain oder E-Mail-Adresse vorhanden ist, wird eine Antwort gesendet, anderenfalls nicht.

Die `.vacation.filter`-Datei kann folgende Einträge enthalten:

```
company.com
mydomain.com
onefriend@hisisp.com
anotherfriend@herisp.com
```

Beachten Sie, dass jede Zeile eine Domain oder eine E-Mail-Adresse enthält. Jeder Eintrag muss sich in einer separaten Zeile befinden. Damit eine E-Mail-Adresse eines Absenders zu einem E-Mail-Adresseintrag passt, muss sie genau mit dem E-Mail-Adresseintrag übereinstimmen (Groß- und Kleinschreibung wird nicht beachtet). Es ist unerheblich, ob die Buchstaben in der Adresse des Absenders Groß- oder Kleinbuchstaben sind. Damit eine E-Mail-Adresse eines Absenders mit einem Domaineintrag übereinstimmt, muss die betreffende Domain in der Adresse des Absender enthalten sein. Beispielsweise stimmen `somebody@dept.company.com` und `someone@company.com` mit dem Domaineintrag `company.com` überein.

Weitere Informationen finden Sie auf der Manpage `vacation(1)`.

Inhalt des `/usr/bin`-Verzeichnisses

Die folgende Tabelle zeigt den Inhalt des `/usr/bin`-Verzeichnisses, das für Mailservices verwendet wird.

Name	Typ	Beschreibung
`aliasadm`	Datei	Ein Programm zum Bearbeiten der NIS+Alias-Maps
`mail`	Datei	Ein Benutzeragent
`mailcompat`	Datei	Ein Filter zum Speichern von Mails im Mailbox-Format von SunOS 4.1
`mailq`	Datei	Ein Programm zum Auflisten des Inhalts einer Mailwarteschlange

Name	Typ	Beschreibung
`mailstats`	Datei	Ein Programm zum Lesen von Mailstatistiken, die in der `/etc/mail/statistics`-Datei gespeichert werden (sofern diese Datei vorhanden ist)
`mailx`	Datei	Ein Benutzeragent
`mconnect`	Datei	Ein Programm, das eine Verbindung mit dem Mailer herstellt, damit Adressen verifiziert und Fehlersuchvorgänge ausgeführt werden können
`praliases`	Datei	Ein Befehl zum Dekompilieren der Aliasdatenbank Informationen zum Dekomplieren finden Sie auf der Manpage für `praliases(1)`.
`rmail`	Symbolische Verknüpfung	Eine symbolische Verknüpfung, die auf `/usr/bin/mail` verweist. Ein Befehl, der oft verwendet wird, um nur das Senden von Mails zuzulassen.
`vacation`	Datei	Ein Befehl zum Einrichten einer automatischen Antwort auf Mails

Inhalt des `/etc/mail`-Verzeichnisses

Die folgende Tabelle zeigt den Inhalt des `/etc/mail`-Verzeichnisses.

Name	Typ	Beschreibung
`Mail.rc`	Datei	Standardeinstellungen für den `mailx`-Benutzeragenten
`aliases`	Datei	Informationen zur Weiterleitung von Mails
`aliases.db`	Datei	Standardmäßige binäre Form von Mail-Weiterleitungsinformationen, die erstellt werden, wenn `newaliases` ausgeführt wird
`aliases.dir`	Datei	Binäre Form von Mail-Weiterleitungsinformationen, die erstellt werden, wenn `newaliases` ausgeführt wird. Kann weiterhin verwendet werden, wird aber ab Solaris 9 nicht mehr standardmäßig verwendet.
`aliases.pag`	Datei	Binäre Form von Mail-Weiterleitungsinformationen, die erstellt werden, wenn `newaliases` ausgeführt wird. Kann weiterhin verwendet werden, wird aber ab Solaris 9 nicht mehr standardmäßig verwendet.
`mailx.rc`	Datei	Standardeinstellungen für den `mailx`-Benutzeragenten

Name	Typ	Beschreibung
`main.cf`	Symbolischer Link	Eine symbolische Verknüpfung von dieser Musterkonfigurationsdatei für Hauptsysteme, die auf `sendmail.cf` verweist, wird für Abwärtskompatibilität bereitgestellt. Diese Datei wird in Version 8.13 von `sendmail` nicht benötigt.
`relay-domains`	Datei	Liste aller Domains, für die eine Weiterleitung zugelassen ist. Standardmäßig ist nur die lokale Domain zugelassen.
`sendmail.cf`	Datei	Konfigurationsdatei für Mail-Routing
`submit.cf`	Datei	Neue Konfigurationsdatei für das MSP (Mail Submission Program, Mailübergabeprogramm). Weitere Informationen finden Sie unter „`submit.cf`-Konfigurationsdatei der Version 8.12 von `sendmail`“ auf Seite 401.
`local-host-names`	Datei	Eine optionale Datei, die Sie erstellen können, wenn die Anzahl der Aliase für den Mailhost zu groß ist
`helpfile`	Datei	Eine Hilfedatei, die vom SMTP-`HELP`-Befehl verwendet wird
`sendmail.pid`	Datei	Eine Datei, die die PID des überwachenden Dämons auflistet und jetzt in `/var/run` zu finden ist
`statistics`	Datei	`sendmail`-Statistikdatei. Wenn diese Datei vorhanden ist, protokolliert `sendmail` das Verkehrsvolumen mithilfe der jeweiligen Mailer. Diese Datei hieß früher `sendmail.st`.
`subsidiary.cf`	Symbolische Verknüpfung	Eine symbolische Verknüpfung, die von dieser Musterkonfigurationsdatei für untergeordnete Systeme auf `sendmail.cf` verweist und für Abwärtskompatibilität bereitgestellt wird. Diese Datei wird in Version 8.13 von `sendmail` nicht benötigt.
`trusted-users`	Datei	Eine Datei, die vertrauenswürdige Benutzer (einen pro Zeile) auflistet, denen gestattet ist, bestimmte Mail-Vorgänge auszuführen. Standardmäßig ist nur `root` in dieser Datei enthalten. Wenn bestimmte Mail-Vorgänge von vertrauenswürdigen Benutzern ausgeführt werden, wird die Warnung `X-Authentication-Warning: header being added to a message` ausgegeben.

Inhalt des `/etc/mail/cf`-Verzeichnisses

Im `/etc/mail`-Verzeichnis befindet sich ein Unterverzeichnis, `cf`, das alle Dateien enthält, die benötigt werden, um eine `sendmail.cf`-Datei zu erstellen. Der Inhalt von `cf` wird in Tabelle 14–9 angezeigt.

Um ab Solaris 10 ein schreibgeschütztes `/usr`-Dateisystem zu unterstützen, wurde der Inhalt des `/usr/lib/mail`-Verzeichnisses in das `/etc/mail/cf`-Verzeichnis verschoben. Beachten Sie jedoch die folgenden Ausnahmen: Die Shell-Skripten `/usr/lib/mail/sh/check-hostname` und `/usr/lib/mail/sh/check-permissions` befinden sich jetzt im Verzeichnis `/usr/sbin`. Lesen Sie dazu „Weitere Dateien, die für Mailservices verwendet werden“ auf Seite 372. Zwecks Abwärtskompatibilität wurden symbolische Verknüpfungen erstellt, die auf die neuen Speicherorte der Dateien verweisen.

TABELLE 14–9 Für Mailservices verwendeter Inhalt des `/etc/mail/cf` -Verzeichnisses

Name	Typ	Beschreibung
`README`	Datei	Beschreibt die Konfigurationsdateien.
`cf/main.cf`	Symbolische Verknüpfung	In Solaris 10 ist dieser Dateiname mit `cf/sendmail.cf` verknüpft. Diese Datei wurde als Hauptkonfigurationsdatei verwendet.
`cf/main.mc`	Symbolische Verknüpfung	In Solaris 10 ist dieser Dateiname mit `cf/sendmail.mc` verknüpft. Diese Datei wurde zum Erstellen der Hauptkonfigurationsdatei verwendet.
`cf/Makefile`	Datei	Enthält Regeln für das Erstellen von neuen Konfigurationsdateien.
`cf/submit.cf`	Datei	Die Konfigurationsdatei für das MSP (Mail Submission Program, Mailübergabeprogramm), das zur Übergabe von Nachrichten dient
`cf/submit.mc`	Datei	Die Datei, die zum Erstellen der `submit.cf`-Datei verwendet wird. Die Datei definiert `m4`-Makros für das MSP (Mail Submission Program, Mailübergabeprogramm).
`cf/sendmail.cf`	Datei	Die Hauptkonfigurationsdatei für sendmail
`cf/sendmail.mc`	Datei	Enthält die `m4`-Makros, die verwendet werden, um die `sendmail.cf`-Datei zu generieren.
`cf/subsidiary.cf`	Symbolische Verknüpfung	In Solaris 10 ist dieser Dateiname mit `cf/sendmail.cf` verknüpft. Diese Datei wurde als Konfigurationsdatei für Hosts verwendet, die `/var/mail` über NFS von einem anderen Host einhängen.

TABELLE 14–9 Für Mailservices verwendeter Inhalt des `/etc/mail/cf` -Verzeichnisses *(Fortsetzung)*

Name	Typ	Beschreibung
`cf/subsidiary.mc`	Symbolische Verknüpfung	In Solaris 10 ist dieser Dateiname mit `cf/sendmail.mc` verknüpft. Diese Datei enthielt die `m4`-Makros, die verwendet wurden, um die `subsidiary.cf`-Datei zu generieren.
`domain`	Verzeichnis	Enthält Beschreibungen zu standortabhängigen Teildomains.
`domain/generic.m4`	Datei	Die generische Domaindatei von Berkeley Software Distribution
`domain/solaris-antispam.m4`	Datei	Die Domaindatei mit Änderungen, die bewirken, dass `sendmail` wie die früheren Solaris-Versionen von `sendmail` funktioniert. Jedoch ist die Weiterleitung komplett deaktiviert, und Absenderadressen ohne Hostname sowie nicht auflösbare Domains werden zurückgewiesen.
`domain/solaris-generic.m4`	Datei	Die standardmäßige Domaindatei mit Änderungen, die bewirken, dass `sendmail` wie die früheren Solaris-Versionen von `sendmail` funktioniert.
`feature`	Verzeichnis	Enthält Definitionen von spezifischen Funktionen für bestimmte Hosts. Eine vollständige Beschreibung der Funktionen finden Sie in der Datei `README`.
`m4`	Verzeichnis	Enthält standortunabhängige include-Dateien.
`mailer`	Verzeichnis	Enthält Definitionen von Mailern, darunter `local`, `smtp` und `uucp`
`main-v7sun.mc`	Datei	Veraltet: In Solaris 10 ist dieser Dateiname in `cf/sendmail.mc` umbenannt.
`ostype`	Verzeichnis	Beschreibt verschiedene Betriebssystemumgebungen-
`ostype/solaris2.m4`	Datei	Definiert den standardmäßigen lokalen Mailer als `mail.local`.
`ostype/solaris2.ml.m4`	Datei	Definiert den standardmäßigen lokalen Mailer als `mail.local`.
`ostype/solaris2.pre5.m4`	Datei	Definiert den lokalen Mailer als `mail`.

TABELLE 14–9 Für Mailservices verwendeter Inhalt des `/etc/mail/cf` -Verzeichnisses *(Fortsetzung)*

Name	Typ	Beschreibung
`ostype/solaris8.m4`	Datei	Definiert den lokalen Mailer als `mail.local` (im LMTP-Modus), aktiviert IPv6 und gibt `/var/run` als Verzeichnis für die `sendmail.pid`-Datei an.
`subsidiary-v7sun.mc`	Datei	Veraltet: In Solaris 10 ist dieser Dateiname in `cf/sendmail.mc` umbenannt.

Inhalt des `/usr/lib`-Verzeichnisses

Die folgende Tabelle zeigt den Inhalt des `/usr/lib`-Verzeichnisses, das für Mailservices verwendet wird.

TABELLE 14–10 Inhalt des `/usr/lib`-Verzeichnisses

Name	Typ	Beschreibung
`mail.local`	Datei	Mailer, der Mails an Mailboxen übermittelt
`sendmail`	Datei	Routing-Programm, auch bekannt als Mail Transfer Agent
`smrsh`	Datei	Shell-Programm (eingeschränkte sendmail-Shell), das die `"|program"`-Syntax von `sendmail` verwendet, um die von `sendmail` ausführbaren Programme auf die Programme zu beschränken, die im `/var/adm/sm.bin` -Verzeichnis aufgelistet sind. Weitere Informationen finden Sie auf der Manpage `smrsh(1M)`. Dort finden Sie Empfehlungen zu Daten, die in `/var/adm/sm.bin` eingefügt werden sollten. Zur Aktivierung fügen Sie diesen `m4`-Befehl, `FEATURE('smrsh')` in Ihre `mc`-Datei ein.
`mail`	Symbolische Verknüpfung	Eine symbolische Verknüpfung verweist auf das `/etc/mail/cf`-Verzeichnis. Weitere Informationen finden Sie unter „Inhalt des `/etc/mail/cf`-Verzeichnisses“ auf Seite 369.

Weitere Dateien, die für Mailservices verwendet werden

Es werden mehrere weitere Dateien und Verzeichnisse für Mailservices verwendet (siehe Tabelle 14–11).

TABELLE 14–11 Weitere Dateien, die für Mailservices verwendet werden

Name	Typ	Beschreibung
`/etc/default/sendmail`	Datei	Listet die Umgebungsvariablen für das Startskript für `sendmail` auf.
`/etc/shells`	Datei	Listet die gültigen Anmelde-Shells auf.
`/etc/mail/cf/sh`	Verzeichnis	Enthält Shell-Skripten, die vom `m4`-Erstellungsprozess und von Umstellungshilfen verwendet werden.
`/usr/sbin/check-permissions`	Datei	Überprüft Berechtigungen von `:include:`-Aliasen und `.forward`-Dateien und den zugehörigen übergeordneten Verzeichnispfad, um für die richtigen Berechtigungen zu sorgen.
`/usr/sbin/check-hostname`	Datei	Überprüft, ob `sendmail` den voll qualifizierten Hostnamen bestimmen kann.
`/usr/sbin/editmap`	Datei	Dient zur Abfrage und Bearbeitung von einzelnen Datensätzen in den Datenbank-Maps für `sendmail`.
`/usr/sbin/in.comsat`	Datei	Mail-Benachrichtigungsdämon
`/usr/sbin/makemap`	Datei	Erstellt binäre Formen von verschlüsselten Maps.
`/usr/sbin/newaliases`	Symbolische Verknüpfung	Eine symbolische Verknüpfung, die auf `/usr/lib/sendmail` verweist. Wird verwendet, um die binäre Form einer Aliasdatenbank zu erstellen. Früher in `/usr/bin`.
`/usr/sbin/syslogd`	Datei	Fehlermeldungsprotokollfunktion, die von `sendmail` verwendet wird
`/usr/sbin/etrn`	Datei	Perl-Skript zum Starten der clientseitigen Remote-Mailwarteschlange
`/usr/dt/bin/dtmail`	Datei	CDE-Mail-Benutzeragent
`/var/mail/`*mailbox1*, `/var/mail/`*mailbox2*	Datei	Mailboxen für übermittelte Mails
`/var/spool/clientmqueue`	Verzeichnis	Speicher für Mails, die vom Clientdämon übermittelt werden
`/var/spool/mqueue`	Verzeichnis	Speicher für Mail, die vom Master-Dämon übermittelt werden

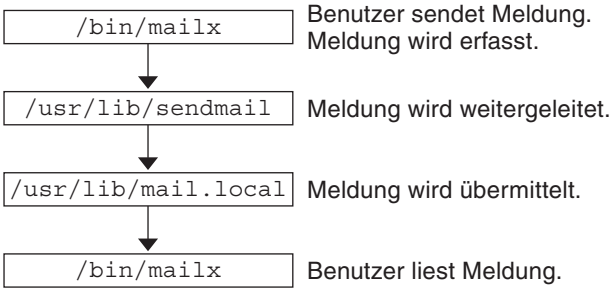
TABELLE 14–11 Weitere Dateien, die für Mailservices verwendet werden *(Fortsetzung)*

Name	Typ	Beschreibung
`/var/run/sendmail.pid`	Datei	Eine Datei, die die PID des überwachenden Dämons auflistet

Interaktionen von Mailprogrammen

Mailservices werden von folgenden Programmen bereitgestellt, die, wie in Abbildung 14–2 dargestellt, interagieren.

ABBILDUNG 14–2 Interaktionen von Mailprogrammen



Es folgt eine Beschreibung der Interaktionen von Mailprogrammen.

1. Benutzer versenden Mails mithilfe von Programmen wie `mailx`. Weitere Informationen finden Sie auf der Manpage `mailx(1)`.
2. Die Mail wird von dem Programm erfasst, das die Mail generiert hat. Anschließend wird die Mail an den `sendmail`-Dämon weitergegeben.
3. Der `sendmail`-Dämon *analysiert* die in der Mail enthaltenen Adressen (d. h., die Adressen werden in identifizierbare Segmente aufgeteilt). Der Dämon verwendet Informationen aus der Konfigurationsdatei `/etc/mail/sendmail.cf`, um die Syntax des Netzwerknamens, Aliase, Weiterleitungsinformationen und die Netzwerktopologie zu bestimmen. Mithilfe dieser Informationen bestimmt `sendmail`, wohin eine Mail weitergeleitet wird, um zum Empfänger zu gelangen.
4. Der `sendmail`-Dämon leitet die Mail zum entsprechenden System weiter.
5. Das `/usr/lib/mail.local`-Programm auf dem lokalen System übermittelt die Mail an die Mailbox im `/var/mail/` *username*-Verzeichnis des Empfängers der Mail.
6. Der Empfänger wird informiert, dass die Mail eingegangen ist. Anschließend ruft der Empfänger die Mail mithilfe von `mail`, `mailx` oder einem ähnlichen Programm ab.

sendmail-Programm

In der folgenden Liste werden einige der Fähigkeiten des sendmail-Programms beschrieben.

- sendmail kann verschiedene Typen von Kommunikationsprotokollen verwenden, beispielsweise TCP/IP und UUCP.
- sendmail implementiert einen SMTP-Server, Mailwarteschlangen und Mailing-Listen.
- sendmail steuert die Interpretierung von Namen mithilfe eines Abgleichsystems, um den folgenden Naming-Konventionen zu entsprechen.
  - Domain-basierte Naming-Konvention. Die Domaintechnik trennt das physische vom logischen Naming. Weitere Informationen zu Domains finden Sie unter „Mailadressen“ auf Seite 358.
  - Verbesserte Methoden, wie beispielsweise die Bereitstellung von Netzwerknamen, die für Hosts in anderen Netzwerke als logische Netzwerknamen sichtbar sind
  - Beliebige (ältere) Naming-Syntaxen
  - Verschiedene Naming-Schemata

Das Betriebssystem Solaris verwendet das sendmail-Programm als Mailrouter. In der folgenden Liste werden einige der Funktionen des Programms beschrieben.

- sendmail empfängt und übermittelt E-Mails an einen lokalen Delivery Agent wie beispielsweise mail.local oder procmail.
- sendmail ist ein Mail Transfer Agent, der Mails von anderen Benutzeragenten (beispielsweise mailx und Mozilla Mail) akzeptiert und die Mails über das Internet zu ihrem Ziel weiterleitet.
- sendmail steuert E-Mail-Nachrichten, die Benutzer auf folgende Weise versenden:
  - Durch Auswertung der Adressen der Empfänger
  - Durch Auswahl eines geeigneten Übermittlungsprogramms
  - Durch Umschreiben der Adressen in ein Format, das vom Delivery Agent verarbeitet werden kann
  - Durch bedarfsweises Umformatieren der Mail-Kopfzeilen
  - Durch Weitergabe der umgewandelten Mail an das Übermittlungsprogramm

Die folgenden Themen enthalten weitere Informationen zum sendmail-Programm.

- „sendmail und seine Umleitungsmechanismen“ auf Seite 376
- „Funktionen und Merkmale von sendmail“ auf Seite 377
- „sendmail-Konfigurationsdatei“ auf Seite 378

`sendmail` und seine Umleitungsmechanismen

Das `sendmail`-Programm unterstützt drei Mechanismen zur Umleitung von Mails. Welchen Mechanismus Sie wählen, hängt von der Art der damit verbundenen Änderung ab.

- Eine Serveränderung
- Eine Domain-übergreifende Änderung
- Eine Änderung, die einen Benutzer betrifft

Außerdem kann der von Ihnen gewählte Umleitungsmechanismus die benötigte Verwaltungsebene beeinflussen. Berücksichtigen Sie die folgenden Optionen.

1. Einer der Umleitungsmechanismen ist *Aliasing*.

   Aliasing ermöglicht eine server- oder Name Service-übergreifende Zuordnung von Namen zu Adressen, je nach Dateityp, den Sie verwenden.

   Berücksichtigen Sie die folgenden Vor- und Nachteile des Name Service-Aliasing.

   - Durch die Verwendung einer Name Service-Aliasdatei können Mail-Umleitungsänderungen von einem einzigen Punkt aus verwaltet werden. Allerdings kann das Name Service-Aliasing eine zeitliche Verzögerung verursachen, wenn eine Umleitungsänderung weitergegeben wird.
   - Die Name Service-Verwaltung ist normalerweise nur bestimmten Systemadministratoren vorbehalten. Ein normaler Benutzer würde diese Datei nicht verwalten.

   Berücksichtigen Sie die folgenden Vor- und Nachteile der Verwendung einer Server-Aliasdatei.

   - Durch Verwenden eine Server-Aliasdatei kann die Umleitung von jeder Person durchgeführt werden, die sich als `root`-Benutzer beim betreffenden Server anmelden kann.
   - Das Server-Aliasing führt in der Regel zu einer geringen oder keiner zeitlichen Verzögerung, wenn eine Umleitungsänderung weitergegeben wird.
   - Die Änderung betrifft nur den lokalen Server, was keine Probleme verursacht, wenn der größte Teil der Mails an einen einzelnen Server gesendet wird. Wenn Sie diese Änderung jedoch auf viele Mailserver übertragen müssen, verwenden Sie einen Name Service.
   - Ein normaler Benutzer würde diese Änderung nicht vornehmen.

   Weitere Informationen finden Sie in diesem Kapitel unter „Mail-Aliasdateien“ auf Seite 379. Eine Übersicht der Schritte finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

2. Der nächste Mechanismus ist *Weiterleitung*.

   Dieser Mechanismus gestattet Benutzern, Mails umzuleiten. Lokale Benutzer können ihre eingehenden Mails auf Folgendes umleiten:

   - Eine andere Mailbox

- Einen anderen Mailer
- Einen anderen Mailhost

Dieser Mechanismus wird durch die Verwendung von `.forward`-Dateien unterstützt. Weitere Informationen zu diesen Dateien finden Sie in diesem Kapitel unter „`.forward`-Dateien“ auf Seite 382. Eine Übersicht der Schritte finden Sie unter „Verwalten von `.forward`-Dateien (Übersicht der Schritte)“ auf Seite 339 in Kapitel 13, „Mailservices (Aufgaben)“.

3. Der letzte Umleitungsmechanismus ist *Einbeziehung*.

   Dieser Mechanismus erlaubt Benutzern, eine Aliasliste zu verwalten, anstatt sich als `root`-Benutzer anmelden zu müssen. Um diese Funktion nutzen zu können, muss der `root`-Benutzer einen entsprechenden Eintrag in der Aliasdatei auf dem Server erstellen. Sobald der Eintrag erstellt ist, kann der Benutzer je nach Bedarf Mails umleiten. Weitere Informationen zur Einbeziehung finden Sie in diesem Kapitel unter „`/etc/mail/aliases`-Datei“ auf Seite 380. Eine Übersicht der Schritte finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

Hinweis – Programme, die Mails lesen, wie beispielsweise `/usr/bin/mailx`, können eigene Aliase haben, die erweitert werden, bevor die Mails `sendmail` erreichen. Die Aliase für `sendmail` können aus Quellen verschiedener Name Services stammen, beispielsweise aus lokalen Dateien, NIS oder NIS+. Die Reihenfolge der Suche wird von der Datei `nsswitch.conf` bestimmt. Weitere Informationen finden Sie auf der Manpage `nsswitch.conf(4)`.

Funktionen und Merkmale von `sendmail`

Das `sendmail`-Programm bietet folgende Funktionen und Merkmale.

- `sendmail` ist zuverlässig. Das Programm dient zur ordnungsgemäßen Übermittlung von Mails. Keine Mail sollte gänzlich verloren gehen.
- `sendmail` verwendet für die Übermittlung die vorhandene Software, soweit dies möglich ist. Beispielsweise kann der Benutzer mit einem Programm interagieren, das Mails generiert und versendet. Wenn eine Mail übermittelt wird, ruft das mailgenerierende Programm `sendmail` auf, das die Mail an die entsprechenden Mailer weiterleitet. Da es sich bei manchen Absendern um Netzwerkserver und bei manchen Mailern um Netzwerkclients handelt, ist es möglich, `sendmail` als Internet-Mailgateway einzusetzen. Eine ausführlichere Beschreibung des Prozesses finden Sie unter „Interaktionen von Mailprogrammen“ auf Seite 374.
- `sendmail` kann so konfiguriert werden, dass komplexe Umgebungen, u. a. auch mehrere Netzwerke, verwaltet werden können. `sendmail` prüft den Inhalt sowie die Syntax einer Adresse, um zu bestimmen, welcher Mailer zu verwenden ist.

- `sendmail` verwendet Konfigurationsdateien, um Mailkonfigurationen zu steuern, anstatt dass Konfigurationsinformationen in den Code kompiliert werden müssen.
- Benutzer können ihre eigenen Mailing-Listen verwalten. Außerdem können Benutzer einen eigenen Weiterleitungsmechanismus angeben, ohne die domainübergreifende Aliasdatei zu ändern, die sich normalerweise im Verzeichnis für domainübergreifende Aliase befindet, das von NIS oder NIS+ verwaltet wird.
- Jeder Benutzer kann einen spezifischen Mailer für die Verarbeitung eingehender Mails angeben. Der benutzerdefinierte Mailer kann Funktionen wie beispielsweise die Rückgabe der Mail "Ich bin im Urlaub" bereitstellen. Weitere Informationen finden Sie auf der Manpage `vacation(1)`.
- `sendmail` legt die Adressen auf einem einzigen Host ab, um den Netzwerkverkehr zu verringern.

`sendmail`-Konfigurationsdatei

Eine *Konfigurationsdatei* bestimmt, wie `sendmail` seine Funktionen ausführt. Die Konfigurationsdatei definiert die Auswahl der Delivery Agents, der Adressumschreibungsregeln und des Formats der Mail-Kopfzeile. Das `sendmail`-Programm verwendet die Informationen aus der Datei `/etc/mail/sendmail.cf`, um ihre Funktionen auszuführen.

Das Betriebssystem Solaris stellt zwei standardmäßige Konfigurationsdateien im `/etc/mail`-Verzeichnis bereit.

1. `sendmail.cf`, eine Konfigurationsdatei, die verwendet wird, um `sendmail` im Dämonmodus auszuführen.
2. `submit.cf`, eine Konfigurationsdatei, die verwendet wird, um `sendmail` im Modus des Mail-Übergabeprogramms anstelle des Dämonmodus auszuführen. Weitere Informationen finden Sie unter „`submit.cf`-Konfigurationsdatei der Version 8.12 von `sendmail`“ auf Seite 401.

Beim Einrichten von Mailclients, Mailservern, Mailhosts oder Mailgateways ist Folgendes zu beachten:

- Bei Mailclients oder Mailservern muss die Standard-Konfigurationsdatei nicht eingerichtet oder bearbeitet werden.
- Um einen Mailhost oder ein Mailgateway einzurichten, müssen Sie Parameter des Relay Mailer und des Relay-Hosts festlegen, die für Ihre Mailkonfiguration benötigt werden. Aufgabenbezogene Informationen finden Sie unter „Einrichten von Mailservices (Übersicht der Schritte)“ auf Seite 304 oder „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“. Beachten Sie, dass bei `sendmail`-Version 8.13 die Datei `main.cf` nicht mehr benötigt wird.

In der folgenden Liste werden einige Konfigurationsparameter beschrieben, die Sie entsprechend den Anforderungen Ihres Standorts ändern können.

- Zeitwerte zur Angabe der folgenden Informationen
  - Zeitüberschreitung bei Lesevorgängen
  - Zeit, die eine nicht übermittelte Mail in der Warteschlange , bevor die Nachricht an den Absender zurückgegeben wird. Lesen Sie dazu „Zusätzliche Warteschlangenfunktionen ab Version 8.12 von `sendmail`“ auf Seite 414. Eine Übersicht der Schritte finden Sie unter „Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)“ auf Seite 336.
- Übermittlungsmodi, die bestimmen, wie schnell Mails übermittelt werden
- Lastgrenzen zur Erhöhung der Effizienz bei starkem Datenverkehr. Diese Parameter verhindern, dass `sendmail` umfangreiche Nachrichten an viele Empfänger übermittelt und dass Nachrichten an Standorte übermittelt werden, die seit längerem außer Betrieb sind.
- Protokollebene zur Angabe der Probleme, die protokolliert werden.

Mail-Aliasdateien

Sie können eine der folgenden Dateien, Maps oder Tabellen verwenden, um Aliase zu verwalten.

- „`.mailrc`-Aliase“ auf Seite 379
- „`/etc/mail/aliases`-Datei“ auf Seite 380
- „`aliases`-NIS-Map“ auf Seite 381
- „NIS+-Tabelle `mail_aliases`“ auf Seite 382

Ihre Methode zur Verwaltung von Aliasen hängt davon ab, welche Personen den Alias verwenden und welche Personen die Möglichkeit haben müssen, den Alias zu ändern. Jeder Alias hat eindeutige Formatanforderungen.

Aufgabenbezogene Informationen finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

`.mailrc`-Aliase

Auf Aliase, die in einer `.mailrc`-Datei aufgelistet sind, kann nur der Benutzer zugreifen, der im Besitz dieser Datei ist. Diese Beschränkung ermöglicht Benutzern, eine Aliasdatei zu erstellen, die sie definieren können und die nur vom Eigentümer verwendet werden kann. Aliase in einer `.mailrc`-Datei haben das folgende Format:

`alias` *aliasname value value value* `...`

aliasname ist der Name, den Benutzer zum Senden von Mails verwenden, und *value* ist eine gültige E-Mail-Adresse.

Wenn ein Benutzer einen persönlichen Alias für `scott` einrichtet, der nicht mit der E-Mail-Adresse für `scott` im Name Service übereinstimmt, tritt ein Fehler auf. Die Mail wird

an die falsche Person weitergeleitet, wenn eine Person versucht, auf eine Mail zu antworten, die von diesem Benutzer generiert wurde. Die einzige Problemumgehung besteht darin, einen anderen Aliasing-Mechanismus zu verwenden.

`/etc/mail/aliases`-Datei

Ein Alias, das in der `/etc/mail/aliases`-Datei eingerichtet wird, kann von jedem Benutzer verwendet werden, der den Namen des Alias und den Hostnamen des Systems kennt, in dem die Datei enthalten ist. Verteilungslistenformate in einer lokalen `/etc/mail/aliases`-Datei haben das folgende Format:

aliasname: *value,value,value* ...

aliasname ist der Name, den Benutzer zum Senden von Mails an diesen Alias verwenden, und *value* ist eine gültige E-Mail-Adresse.

Wenn Ihr Netzwerk keinen Name Service ausführt, muss die `/etc/mail/aliases` -Datei jedes Systems Einträge für alle Clients enthalten. Sie können entweder die Datei auf jedem System bearbeiten oder die Datei auf einem System bearbeiten und dann in jedes der anderen Systeme kopieren.

Die Aliase in der `/etc/mail/aliases`-Datei werden in Textform gespeichert. Wenn Sie die `/etc/mail/aliases`-Datei bearbeiten, müssen Sie das `newaliases`-Programm ausführen. Dieses Programm kompiliert die Datenbank neu und macht die Aliase in binärer Form für das `sendmail`-Programm verfügbar. Aufgabenbezogene Informationen finden Sie unter „So richten Sie eine lokale Mailaliasdatei ein“ auf Seite 331 in Kapitel 13, „Mailservices (Aufgaben)“. Sie können auch die Mailing-Listen-Funktion in der Solaris Management Console verwenden, um die Mailaliase zu verwalten, die in den lokalen `/etc`-Dateien gespeichert sind.

Sie können Aliase nur für lokale Namen erstellen, beispielsweise einen aktuellen Hostnamen oder keinen Hostnamen. Beispielsweise würde ein Aliaseintrag für den Benutzer `ignatz`, der eine Mailbox auf dem System `saturn` hat, den folgenden Eintrag in der `/etc/mail/aliases`-Datei haben:

```
ignatz: ignatz@saturn
```

Sie sollten eine Verwaltungskonto für jeden Mailserver erstellen. Sie erstellen ein solches Konto, indem Sie eine Mailbox, die sich auf dem Mailserver befindet, `root` zuweisen und einen Eintrag für `root` in die `/etc/mail/aliases`-Datei einfügen. Wenn beispielsweise das System `saturn` ein Mailboxserver ist, fügen Sie den Eintrag `root: sysadmin@saturn` in die `/etc/mail/aliases` -Datei ein.

Normalerweise kann nur der `root`-Benutzer diese Datei bearbeiten. Wenn Sie jedoch die Solaris Management Console verwenden, können alle Benutzer in Gruppe 14 (Systemverwaltungsgruppe) die lokale Datei ändern. Eine weitere Möglichkeit besteht darin, den folgenden Eintrag zu erstellen:

aliasname: `:include:`*/path/aliasfile*

aliasname ist der Name, den der Benutzer verwendet, um Mails zu versenden, und */path/aliasfile* ist der vollständige Pfad zu der Datei, die die Aliasliste enthält. Die Aliasdatei sollt E-Mail-Einträge enthalten, und zwar einen Eintrag pro Zeile und keine anderen Notationen.

user1@host1
user2@host2

Sie können zusätzliche Maildateien in `/etc/mail/aliases` definieren, um ein Protokoll zu führen oder eine Sicherungskopie zu erstellen. Mit dem folgenden Eintrag werden alle Mails, die an *aliasname* gesendet werden, in *filename* gespeichert.

aliasname: `/home/backup/`*filename*

Sie können Mails auch an einen anderen Prozess weiterleiten. Im folgenden Beispiel wird eine Kopie der Mail in *filename* gespeichert und eine Kopie ausgedruckt.

aliasname: `"|tee -a /home/backup/`*filename* `|lp"`

Eine Übersicht der Schritte finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

`aliases`-NIS-Map

Alle Benutzer in einer lokalen Domain können die Einträge verwenden, die sich in der NIS-Map `aliases` befinden. Der Grund dafür ist der, dass das `sendmail`-Programm die NIS-Map `aliases` anstelle der lokalen `/etc/mail/aliases`-Dateien verwenden kann, um Mailadressen zu bestimmen. Weitere Informationen finden Sie auf der Manpage `nsswitch.conf(4)`.

Aliase in der NIS-Map `aliases` haben das folgende Format:

aliasname: *value,value,value* ...

aliasname ist der Name, den Benutzer zum Senden von Mails verwenden, und *value* ist eine gültige E-Mail-Adresse.

Die NIS-Map `aliases` muss Einträge für alle Mailclients enthalten. Im Allgemeinen kann nur der Root-Benutzer auf dem NIS-Master diese Einträge ändern. Dieser Aliastyp eignet sich möglicherweise nicht für Aliase, die sich ständig ändern. Solche Aliase können jedoch hilfreich sein, wenn die Aliase auf eine andere Datei verweisen wie in dem folgenden Syntaxbeispiel:

aliasname: *aliasname@host*

aliasname ist der Name, den Benutzer zum Senden von Mails verwenden, und *host* ist der Hostname für den Server, der eine `/etc/mail/alias`-Datei enthält.

Aufgabenbezogene Informationen finden Sie unter „So richten Sie eine `mail.aliases`-NIS-Map ein“ auf Seite 330 in Kapitel 13, „Mailservices (Aufgaben)“.

NIS+-Tabelle `mail_aliases`

Die NIS+-Tabelle `mail_aliases` enthält die Namen, unter denen ein System oder eine Person in der lokalen Domain bekannt ist. Das `sendmail`-Programm kann die NIS+-Tabelle `mail_aliases` anstelle der lokalen `/etc/mail/aliases`-Dateien verwenden, um E-Mail-Adressen zu bestimmen. Weitere Informationen finden Sie auf den Manpages `aliasadm(1M)` und `nsswitch.conf(4)`.

Aliase in der NIS+-Tabelle `mail_aliases` haben das folgende Format:

alias: *expansion* # ["*options*" # "*comments*"]

In Tabelle 14–12 werden vier Spalten beschrieben, die in einer NIS+-Tabelle `mail_aliases` enthalten sind.

TABELLE 14–12 Spalten in der NIS+-Tabelle `mail_aliases`

Spalte	Beschreibung
`alias`	Der Name des Alias
`expansion`	Der Wert des Alias oder einer Liste von Aliasen in einer `sendmail` `/etc/mail/aliases`-Datei
`options`	Die Spalte, die für die spätere Verwendung reserviert ist
`comments`	Die Spalte für Kommentare zu einem bestimmten Alias

Die NIS+-Tabelle `mail_aliases` muss Einträge für alle Mailclients enthalten. Sie können Einträge in der NIS+-Tabelle `aliases` mit dem Befehl `aliasadm` auflisten, erstellen, modifizieren und löschen. Um den Befehl `aliasadm` verwenden zu können, müssen Sie ein Mitglied der NIS+-Gruppe sein, die im Besitz der `aliases`-Tabelle ist. Aufgabenbezogene Informationen finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“. Sie können auch die Solaris Management Console verwenden, um die NIS+-Mailaliase zu verwalten.

Hinweis – Um eine neue NIS+-Tabelle `aliases` zu erstellen, müssen Sie die Tabelle zunächst initialisieren. Anschließend erstellen Sie die Einträge. Ist die Tabelle bereits vorhanden, wird keine Initialisierung benötigt.

`.forward`-Dateien

Benutzer können eine `.forward`-Datei in ihren Home-Verzeichnissen erstellen, die von `sendmail` und anderen Programmen verwendet werden kann, um Mails umzuleiten oder zu senden. Relevante Informationen finden Sie unter:

- „Vermeidbare Situationen“ auf Seite 383

- „Einstellungen für `.forward`-Dateien“ auf Seite 383
- „`.forward.`*hostname*-Datei“ auf Seite 383
- „`.forward+`*detail*-Datei“ auf Seite 384

Eine Übersicht der Schritte finden Sie unter „Verwalten von `.forward`-Dateien (Übersicht der Schritte)“ auf Seite 339 in Kapitel 13, „Mailservices (Aufgaben)“.

Vermeidbare Situationen

In der folgenden Liste werden Situationen beschrieben, die Sie vermeiden oder ohne großen Aufwand korrigieren können.

- Wenn eine Mail nicht wie erwartet an die entsprechende Adresse übermittelt wird, überprüfen Sie die `.forward`-Datei des betreffenden Benutzers. Der Benutzer kann die `.forward`-Datei im Home-Verzeichnis von `host1` abgelegt haben, von wo aus Mails an `user@host2` weitergeleitet werden. Wenn die Mail bei `host2` angekommen ist, sucht `sendmail` in den NIS- oder NIS+-Aliasen nach `user` und sendet die Mail an `user@host1` zurück. Daraus resultieren eine Schleife und mehr zurückgesendete Mails.
- Um Sicherheitsprobleme zu vermeiden, sollten Sie `.forward`-Dateien nie im `root`-Verzeichnis und in `bin`-Konten ablegen. Leiten Sie bei Bedarf die Mails weiter, indem Sie stattdessen die `aliases`-Datei verwenden.

Einstellungen für `.forward`-Dateien

Damit die `.forward`-Dateien zur Effizienz der Mailübermittlung beitragen, stellen Sie sicher, dass die folgenden Einstellungen (meistens Berechtigungsoptionen) richtig eingestellt sind.

- Die `.forward`-Datei darf nur vom Eigentümer der Datei beschrieben werden können. Diese Beschränkung verhindert, dass Benutzer Sicherheitsverstöße begehen.
- Die Pfade, die zum Home-Verzeichnis führen, müssen im Besitz des `root`-Benutzers sein und dürfen nur von diesem beschrieben werden. Wenn sich beispielsweise eine `.forward`-Datei in `/export/home/terry` befindet, müssen `/export` und `/export/home` im Besitz des `root`-Benutzers sein und dürfen nur von diesem beschrieben werden.
- Das aktuelle Home-Verzeichnis sollte nur vom Benutzer beschrieben werden dürfen.
- Die `.forward`-Datei kann keine symbolische Verknüpfung sein und kann nur eine harte Verknüpfung haben.

`.forward.`*hostname*-Datei

Sie können eine `.forward.` *hostname*-Datei zum Umleiten von Mails erstellen, die an einen spezifischen Host gesendet werden. Wenn beispielsweise der Alias eines Benutzers von `sandy@phoenix.example.com` in `sandy@example.com` geändert wurde, legen Sie eine `.forward.phoenix`-Datei im Home-Verzeichnis für `sandy` ab.

```
% cat .forward.phoenix
sandy@example.com
"|/usr/bin/vacation sandy"
% cat .vacation.msg
From: sandy@example.com (via the vacation program)
Subject: my alias has changed

My alias has changed to sandy@example.com.
Please use this alias in the future.
The mail that I just received from you
has been forwarded to my new address.

Sandy
```

In diesem Beispiel können Mails an die richtige Stelle weitergeleitet werden, während der Absender über die Aliasänderung informiert wird. Da das Programm `vacation` nur eine Maildatei zulässt, können Sie nur jeweils eine Mail weiterleiten. Wenn die Mail jedoch nicht hostspezifisch ist, kann eine vacation-Maildatei von `.forward`-Dateien für viele Hosts verwendet werden.

`.forward+`*detail*-Datei

Eine weitere Erweiterung des Weiterleitungsmechanismus ist die `.forward+`*detail*-Datei. Die *detail*-Zeichenfolge kann eine beliebige Zeichenfolge sein. Operatorzeichen dürfen nicht enthalten sein. Die Operatorzeichen sind `.:%&!^[]+`. Wenn Sie diesen Datentyp verwenden, können Sie feststellen, ob jemand Ihre E-Mail-Adresse ohne Ihr Wissen benutzt. Wenn ein Benutzer beispielsweise jemandem mitteilt, die E-Mail-Adresse `sandy+test1@example.com` zu verwenden, hätte der Benutzer die Möglichkeit, jede weitere Mail zu identifizieren, die an diesen Alias übermittelt wird. Jede Mail, die an den Alias `sandy+test1@example.com` gesendet wird, wird standardmäßig mit dem Alias und den `.forward+`*detail*-Dateien abgeglichen. Wenn keine Übereinstimmungen vorhanden sind, wird die Mail an `sandy@example.com` zurückgesendet. Der Benutzer kann dann jedoch eine Änderung in der Mail-Kopfzeile `To:` erkennen.

`/etc/default/sendmail`-Datei

Diese Datei dient zum Speichern von Startoptionen für `sendmail`, damit die Optionen nicht entfernt werden, wenn ein Host aktualisiert wird. Folgende Variablen können verwendet werden:

CLIENTOPTIONS="*string*"
: Wählt zusätzliche Optionen aus, die in Verbindung mit dem Clientdämon verwendet werden. Dieser liest die ausschließlich für Clients vorgesehene Warteschlange (`/var/spool/clientmqueue`) und übernimmt die Funktion eines Clientwarteschlangen-Betriebsprogramms. Da die Syntax nicht geprüft wird, sollten Sie mit Umsicht vorgehen, wenn Sie Änderungen an dieser Variablen vornehmen.

CLIENTQUEUEINTERVAL=#
: Ähnlich der Option `QUEUEINTERVAL` legt `CLIENTQUEUEINTERVAL` das Zeitintervall für die Mailwarteschlangenprozesse fest. Die Option `CLIENTQUEUEINTERVAL` steuert jedoch die Funktionen des Clientdämons und nicht die Funktionen des Master-Dämons. Der Master-Dämon kann normalerweise alle Mails an den SMTP-Port weiterleiten. Wenn jedoch die Maillast zu groß ist oder der Master-Dämon nicht ausgeführt wird, werden die Mails in die ausschließlich für Clients vorgesehene Warteschlange (`/var/spool/clientmqueue`) gestellt. Der Clientdämon, der die ausschließlich für Clients vorgesehene Warteschlange liest, fungiert dann als Clientwarteschlangen-Verarbeitungsprogramm.

ETRN_HOSTS="*string*"
: Ermöglicht einem SMTP-Client und -Server, miteinander zu interagieren, ohne auf die periodischen Warteschlangenprozessintervalle warten zu müssen. Der Server kann sofort den Teil seiner Warteschlange bereitstellen, der an die angegebenen Hosts weitergeleitet wird. Weitere Informationen finden Sie auf der Manpage `etrn(1M)`.

MODE=-bd
: Wählt den Modus zum Starten von `sendmail`. Verwenden Sie die Option `-bd`, oder lassen Sie sie undefiniert.

OPTIONS=*string*
: Wählt zusätzliche Optionen, die in Verbindung mit dem Master-Dämon verwendet werden. Da die Syntax nicht geprüft wird, sollten Sie mit Umsicht vorgehen, wenn Sie Änderungen an dieser Variablen vornehmen.

QUEUEINTERVAL=#
: Legt das Intervall für die Mailwarteschlangenprozesse auf dem Master-Dämon fest. # kann eine positive Ganzzahl sein, nach der entweder `s` (Sekunden), `m` (Minuten), `h` (Stunden), `d` (Tage) oder `w` (Wochen) folgt. Die Syntax wird geprüft, bevor `sendmail` gestartet wird. Wenn das Intervall negativ ist oder der Eintrag nicht mit einem entsprechenden Buchstaben endet, wird das Intervall ignoriert, und `sendmail` wird mit einem Warteschlangenintervall von 15 Minuten gestartet.

QUEUEOPTIONS=p
: Aktiviert ein dauerhaftes Warteschlangen-Betriebsprogramm, das zwischen den Warteschlangenprozessintervallen inaktiv ist, anstatt jeweils ein neues Warteschlangen-Betriebsprogramm für jedes neue Warteschlangenprozessintervall zu aktivieren. Sie können diese Option auf `p`, die einzige verfügbare Einstellung, setzen. Andernfalls ist diese Option nicht aktiviert.

Mailadressen und Mail-Routing

Welchen Pfad eine Mail während der Übermittlung verwendet, hängt von der Konfiguration des Clientsystems und der Topologie der Maildomain ab. Jede zusätzliche Ebene von Mailhosts oder Maildomains kann zu einer weiteren Aliasauflösung führen. Der Routing-Vorgang ist im Grunde auf den meisten Hosts der gleiche.

Sie können ein Clientsystem so konfigurieren, dass es Mails lokal empfangen kann. Wenn Mails lokal empfangen werden, wird `sendmail` im lokalen Modus ausgeführt. Der lokale Modus ist der Standardmodus für alle Mailserver und einige Clients. Auf einem Mailserver oder Mailclient im lokalen Modus wird eine E-Mail auf folgende Weise weitergeleitet.

Hinweis – Das folgende Beispiel setzt voraus, dass Sie die in der `sendmail.cf`-Datei festgelegte standardmäßige Regelliste verwenden.

---

1. Erweitern Sie nach Möglichkeit den Mailalias. Starten Sie dann den lokalen Routing-Prozess neu.

   Die Mailadresse wird erweitert, indem im Name Service nach dem Mailalias gesucht und der neue Wert ersetzt wird, sofern ein neuer Wert gefunden wird. Dieser neue Alias wird anschließend erneut geprüft.
2. Wenn es sich um eine lokale Mail handelt, senden Sie die Mail an `/usr/lib/mail.local` .

   Die Mail wird an eine lokale Mailbox gesendet.
3. Wenn die Mailadresse einen Host in der entsprechenden Maildomain enthält, senden Sie die Mail an den betreffenden Host.
4. Wenn die Adresse keinen Host in der Domain enthält, senden Sie die Mail an den Mailhost.

   Auf dem Mailhost wird der gleiche Routing-Prozess wie auf dem Mailserver ausgeführt. Der Mailhost kann jedoch Mails empfangen, die an den Domainnamen oder an den Hostnamen adressiert sind.

Interaktionen von `sendmail` mit Name Services

In diesem Abschnitt werden Domainnamen und ihre Verwendung in Zusammenhang mit `sendmail` und Name Services beschrieben. Außerdem werden die Regeln für die effektive Verwendung von Name Services und die spezifischen Interaktionen von `sendmail` mit Name Services beschrieben. Ausführliche Informationen finden Sie unter:

- „`sendmail.cf` und Maildomains“ auf Seite 387
- „`sendmail` und Name Services“ auf Seite 387
- „Interaktionen von NIS und `sendmail`“ auf Seite 389
- „Interaktionen von `sendmail` mit NIS und DNS“ auf Seite 389
- „Interaktionen von NIS+ und `sendmail`“ auf Seite 390

- „Interaktionen von sendmail mit NIS+ und DNS“ auf Seite 391

Aufgabenbezogene Informationen finden Sie unter „So verwenden Sie DNS mit sendmail“ auf Seite 312 oder „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

sendmail.cf und Maildomains

Die standardmäßige sendmail.cf-Datei verwendet Maildomains, um zu bestimmen, ob Mails direkt oder über einen Mailhost übermittelt werden. Intradomain-Mails werden über eine direkte SMTP-Verbindung übermittelt, während Interdomain-Mails an einen Mailhost weitergeleitet werden.

In einem gesicherten Netzwerk haben nur wenige ausgewählte Hosts die Berechtigung, Pakete zu generieren, die für externe Ziele bestimmt sind. Selbst wenn ein Host über die IP-Adresse des Remote-Hosts verfügt, der sich außerhalb der Maildomain befindet, ist die Herstellung einer SMTP-Verbindung nicht gewährleistet. Die standardmäßige sendmail.cf-Datei setzt Folgendes voraus:

- Der aktuelle Host ist nicht berechtigt, Pakete direkt an den Host außerhalb der Maildomain zu senden.
- Der Mailhost kann die Mail an einen berechtigten Host senden, der Pakete direkt auf einen externen Host übertragen kann. Der Mailhost kann ein berechtigter Host sein.

Unter diesen Voraussetzungen ist der Mailhost für die Übermittlung oder Weiterleitung von Interdomain-Mails verantwortlich.

sendmail und Name Services

sendmail stellt verschiedene Anforderungen an Name Services. Um Ihr Verständnis bezüglich dieser Anforderungen zu vertiefen, wird in diesem Abschnitt zunächst das Verhältnis zwischen Maildomains und Name Service-Domains beschrieben. Anschließend werden die verschiedenen Anforderungen beschrieben. Weitere Informationen finden Sie unter:

- „Maildomains und Name Service-Domains“ auf Seite 387
- „Anforderungen an Name Services“ auf Seite 388
- Manpages zu NIS+(1), nisaddent(1M) und nsswitch.conf(4)

Maildomains und Name Service-Domains

Der Name der Maildomain muss ein Suffix der Name Service-Domain sein. Wenn beispielsweise der Domainname des Name Service A.B.C.D lautet, kann der Domainname einer der folgenden sein:

- A.B.C.D

- B.C.D
- C.D
- D

Wenn ein Maildomainname erstmals erstellt wird, ist er oft identisch mit der Name Service-Domain. Die Name Service-Domain kann mit zunehmender Größe des Netzwerks in kleinere Teile aufgeteilt werden, sodass der Name Service besser verwaltet werden kann. Jedoch wird die Maildomain oftmals nicht geteilt, um konsistentes Aliasing zu gewährleisten.

Anforderungen an Name Services

In diesem Abschnitt werden die Anforderungen beschrieben, die sendmail an Name Services stellt.

In einem Name Service muss eine Hosttabelle oder Host-Map eingerichtet werden, damit drei Arten von gethostbyname()-Abfragen unterstützt werden.

- mailhost – Manche Name Service-Konfigurationen erfüllen diese Anforderung automatisch.
- Vollständiger Hostname (beispielsweise smith.admin.acme.com) – Viele Name Service-Konfigurationen erfüllen diese Anforderung.
- Kurzer Hostname (beispielsweise smith) – sendmail muss eine Verbindung mit dem Mailhost herstellen, um externe Mails weiterzuleiten. Um festzustellen, ob sich eine Mailadresse in der aktuellen Domain befindet, wird gethostbyname() mit dem vollständigen Hostnamen aufgerufen. Wenn der Eintrag gefunden wird, wird die Adresse als interne Adresse betrachtet.

  NIS, NIS+ und DNS unterstützen gethostbyname() mit einem kurzen Hostnamen als Argument, wodurch diese Anforderung automatisch erfüllt wird.

Zwei zusätzliche Regeln zum Host-Name Service müssen eingehalten werden, um effiziente sendmail-Services innerhalb eines Name Service einzurichten.

- gethostbyname() sollte in Verbindung mit dem Argument des vollständigen Hostnamens und dem Argument des kurzen Hostnamens zu konsistenten Ergebnissen führen. gethostbyname(smith.admin.acme.com) sollte beispielsweise dasselbe Ergebnis wie gethostbyname(smith) erbringen, wenn beide Funktionen von der Maildomain admin.acme.com aus aufgerufen werden.
- Bei allen Name Service-Domains, die zu einer allgemeinen Maildomain gehören, sollte gethostbyname() mit einem kurzen Hostnamen dasselbe Ergebnis erbringen. Wenn beispielsweise die Maildomain smith.admin.acme.com angegeben ist, sollte gethostbyname(smith) dasselbe Ergebnis erbringen, unabhängig davon, ob der Aufruf von der Domain ebb.admin.acme.com oder esg.admin.acme.com aus erfolgt. Der Name der Maildomain ist normalerweise kürzer als der Name der Name Service-Domain. Diese Anforderung ist für die verschiedenen Name Services daher mit bestimmten Konsequenzen verbunden.

Weitere Informationen zur gethostbyname()-Funktion finden Sie auf der Manpage gethostbyname(3NSL).

Interaktionen von NIS und sendmail

In der folgenden Liste werden die Interaktionen von sendmail und NIS beschrieben und Orientierungshilfen bereitgestellt.

- **Maildomainname** – Wenn Sie NIS als primären Name Service einrichten, entfernt sendmail automatisch den ersten Teil des NIS-Domainnamens und verwendet das Ergebnis als Maildomainname. Aus ebs.admin.acme.com wird beispielsweise admin.acme.com.
- **Mailhostname** – In der NIS-Host-Map muss ein mailhost-Eintrag vorhanden sein.
- **Vollständige Hostnamen** – Mithilfe einer normalen NIS-Konfiguration kann kein vollständiger Hostname aufgelöst werden. Anstatt NIS so zu konfigurieren, dass der vollständige Hostname aufgelöst wird, heben Sie diese Anforderung bei sendmail auf, indem Sie die Datei sendmail.cf bearbeiten und alle %l durch %y ersetzen. Durch diese Änderung wird die von sendmail durchgeführte Erkennung von Interdomain-Mails deaktiviert. Wenn der Zielhost in eine IP-Adresse aufgelöst werden kann, wird eine direkte SMTP-Übermittlung unternommen. Stellen Sie sicher, dass Ihre NIS-Host-Map keinen Hosteintrag enthält, der außerhalb der aktuellen Maildomain liegt. Andernfalls müssen Sie die Datei sendmail.cf weiter anpassen.
- **Abgleichen vollständiger Hostnamen und kurzer Hostnamen** – Folgen Sie den vorangegangenen Anweisungen, um gethostbyname() im Zusammenhang mit vollständigen Hostnamen zu deaktivieren.
- **Mehrere NIS-Domains in einer Maildomain** – Alle NIS-Host-Maps, die zu einer allgemeinen Maildomain gehören, müssen dieselben Hosteinträge aufweisen. Die Host-Map in der Domain ebs.admin.acme.com sollte beispielsweise mit der Host-Map in der Domain esg.admin.acme.com übereinstimmen. Anderenfalls könnte eine Adresse in einer NIS-Domain funktionieren, in einer anderen aber nicht.

Aufgabenbezogene Informationen finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

Interaktionen von sendmail mit NIS und DNS

In der folgenden Liste werden die Interaktionen von sendmail mit NIS und DNS beschrieben und Orientierungshilfen bereitgestellt.

- **Maildomainname** – Wenn Sie NIS als primären Name Service einrichten, entfernt sendmail automatisch den ersten Teil des NIS-Domainnamens und verwendet das Ergebnis als Maildomainname. Aus ebs.admin.acme.com wird beispielsweise admin.acme.com.

- **Mailhostname** – Wenn die DNS-Weiterleitungsfunktion aktiviert ist, werden Abfagen, die NIS nicht auflösen kann, an DNS weitergeleitet. Aus diesem Grunde benötigen Sie keinen `mailhost`-Eintrag in der NIS-Host-Map.
- **Vollständige Hostnamen** – DNS kann im Gegensatz zu NIS vollständige Hostnamen auflösen. Diese Anforderung wird erfüllt, wenn Sie das reguläre Verfahren zum Einrichten von NIS und DNS anwenden.
- **Abgleichen vollständiger Hostnamen und kurzer Hostnamen** – Für jeden Hosteintrag in der NIS-Hosttabelle muss ein entsprechender Hosteintrag in DNS vorhanden sein.
- **Mehrere NIS-Domains in einer Maildomain** – Alle NIS-Host-Maps, die zu einer allgemeinen Maildomain gehören, müssen dieselben Hosteinträge aufweisen. Die Host-Map in der Domain `ebs.admin.acme.com` sollte beispielsweise mit der Host-Map in der Domain `esg.admin.acme.com` übereinstimmen. Anderenfalls könnte eine Adresse in einer NIS-Domain funktionieren, in einer anderen aber nicht.

Aufgabenbezogene Informationen finden Sie unter „So verwenden Sie DNS mit `sendmail`“ auf Seite 312 und „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

Interaktionen von NIS+ und `sendmail`

In der folgenden Liste werden die Interaktionen von `sendmail` und NIS+ beschrieben und Orientierungshilfen bereitgestellt.

- **Maildomainname** – Wenn Sie NIS+ als primären Name Service einrichten, kann `sendmail` die Maildomain über die NIS+-Tabelle `sendmailvars` prüfen. Diese NIS+-Tabelle umfasst eine Schlüsselspalte und eine Wertespalte. Um Ihre Maildomain einzurichten, müssen Sie einen Eintrag in diese Tabelle einfügen. In diesem Eintrag sollte die Schlüsselspalte auf die Literalzeichenfolge `maildomain` und die Wertespalte auf Ihren Maildomainnamen gesetzt sein. Beispiel: `admin.acme.com`. Obwohl NIS+ jede beliebige Zeichenfolge in der `sendmailvars`-Tabelle zulässt, gilt weiterhin die Suffixregel, damit das Mailsystem ordnungsgemäß funktioniert. Sie können `nistbladm` verwenden, um den `maildomain`-Eintrag in die `sendmailvars`-Tabelle einzufügen. Beachten Sie beim folgenden Beispiel, dass die Maildomain ein Suffix der NIS+-Domain ist.

  ```
  nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
  ```

- **Mailhostname** – In der NIS+-Hosttabelle muss ein `mailhost`-Eintrag vorhanden sein.
- **Vollständige Hostnamen** – NIS+ kann den vollständigen Hostnamen auflösen. Wenden Sie das reguläre NIS+-Konfigurationsverfahren an, um diese Anforderung zu erfüllen.
- **Abgleichen vollständiger Hostnamen und kurzer Hostnamen** – Um diese Anforderung zu erfüllen, können Sie die Einträge in der Hosttabelle duplizieren. Sie haben auch die Möglichkeit, alle Hosteinträge in den benutzerspezifischen Name Service-Domains in eine Master-Hosttabelle auf der Maildomainebene einzutragen.

- **Mehrere NIS-Domains in einer Maildomain** – Um diese Anforderung zu erfüllen, können Sie die Einträge in allen Hosttabellen duplizieren. Sie haben auch die Möglichkeit, alle Hosteinträge in den benutzerspezifischen Name Service-Domains in eine Master-Hosttabelle auf der Maildomainebene einzutragen. Sie können damit verschiedene logische oder physische Hosttabellen zu einer Hosttabelle zusammenführen. Derselbe Hostname kann dann jedoch nicht mehrfach in den mehreren Name Service-Domains verwendet werden, die gemeinsam eine allgemeine Maildomain nutzen.

Aufgabenbezogene Informationen finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 in Kapitel 13, „Mailservices (Aufgaben)“.

Interaktionen von `sendmail` mit NIS+ und DNS

In der folgenden Liste werden die Interaktionen von `sendmail` mit NIS+ und DNS beschrieben und Orientierungshilfen bereitgestellt.

- **Maildomainname** – Wenn Sie NIS+ als primären Name Service einrichten, kann `sendmail` die Maildomain über die NIS+-Tabelle `sendmailvars` prüfen. Diese NIS+-Tabelle umfasst eine Schlüsselspalte und eine Wertespalte. Um Ihre Maildomain einzurichten, müssen Sie einen Eintrag in diese Tabelle einfügen. In diesem Eintrag sollte die Schlüsselspalte auf die Literalzeichenfolge `maildomain` und die Wertespalte auf Ihren Maildomainnamen gesetzt sein. Beispiel: `admin.acme.com`. Obwohl NIS+ jede beliebige Zeichenfolge in der `sendmailvars`-Tabelle zulässt, gilt weiterhin die Suffixregel, damit das Mailsystem ordnungsgemäß funktioniert. Sie können `nistbladm` verwenden, um den `maildomain`-Eintrag in die `sendmailvars`-Tabelle einzufügen. Beachten Sie beim folgenden Beispiel, dass die Maildomain ein Suffix der NIS+-Domain ist.

  ```
  nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
  ```

- **Mailhost-Hostname** – Wenn Ihr Netzwerk sowohl NIS+ als auch DNS als Quelle für die Hostdatenbank verwendet, Sie können den `mailhost`-Eintrag entweder in der NIS+- oder der DNS-Hosttabelle einfügen. Stellen Sie sicher, dass Ihre Benutzer sowohl NIS+ als auch DNS als Quelle für die Hostdatenbank in die `/etc/nsswitch.conf`-Datei eintragen.
- **Vollständige Hostnamen** – Sowohl NIS+ als auch DNS können vollständige Hostnamen auflösen. Wenden Sie das reguläre NIS+- und DNS-Konfigurationsverfahren an, um diese Anforderung zu erfüllen.
- **Abgleichen vollständiger Hostnamen und kurzer Hostnamen** – Für jeden Hosteintrag in der NIS+-Hosttabelle muss ein entsprechender Hosteintrag in DNS vorhanden sein.
- **Mehrere NIS-Domains in einer Maildomain** – Um diese Anforderung zu erfüllen, können Sie die Einträge in allen Hosttabellen duplizieren. Sie haben auch die Möglichkeit, alle Hosteinträge in den benutzerspezifischen Name Service-Domains in eine Master-Hosttabelle auf der Maildomainebene einzutragen.

Aufgabenbezogene Informationen finden Sie unter „Verwalten von Mailaliasdateien (Übersicht der Schritte)“ auf Seite 323 und „So verwenden Sie DNS mit sendmail“ auf Seite 312 in Kapitel 13, „Mailservices (Aufgaben)“.

Änderungen in Version 8.13 von sendmail

Unter den vielen neuen Funktionen der neuen Version von sendmail ist die Option FallBackSmartHost die wichtigste Neuerung. Aufgrund dieser neuen Option sind die Dateien main.cf und subsidiary.cf nicht mehr erforderlich. Die Datei main.cf kam in Umgebungen zum Einsatz, die MX-Datensätze unterstützen. Die Datei subsidiary.cf wurde in Umgebungen ohne einen vollständig einsatzbereiten DNS verwendet. In solchen Umgebungen wurde ein Smart-Host anstelle von MX-Datensätzen eingesetzt. Mit der Option FallBackSmartHost ist nun eine einheitliche Konfiguration möglich. Diese Option verhält sich wie ein MX-Datensatz der letzten möglichen Vorrangstufe für alle Umgebungen. Aktivieren Sie diese Option, um einen gut verbundenen Host zu gewährleisten, der als Backup oder Failover für alle fehlgeschlagenen MX-Datensätze dient, und um sicherzustellen, dass die Mails an die Clients übermittelt werden.

Weitere Informationen zu Version 8.13 finden Sie in den folgenden Abschnitten:

- „Zusätzliche Befehlszeilenoptionen in Version 8.13 von sendmail“ auf Seite 397
- „Zusätzliche und überarbeitete Konfigurationsdateioptionen in Version 8.13 von sendmail“ auf Seite 398
- „Zusätzliche und überarbeitete FEATURE()-Deklarationen in Version 8.13 von sendmail“ auf Seite 399

Ab Solaris 10 1/06 kann SMTP zudem mit TLS (Transport Layer Security) ausgeführt werden. Weitere Informationen finden Sie in der nachstehenden Beschreibung.

Unterstützung für die Ausführung von SMTP mit TLS in Version 8.13 von sendmail

Die Kommunikation zwischen SMTP-Servern und -Clients wird normalerweise auf keiner Seite kontrolliert oder als vertrauenswürdig betrachtet. Dieser Mangel an Sicherheit erlaubt Dritten, die Kommunikation zwischen einem Server und einem Client zu überwachen oder sogar zu ändern. Ab Solaris 10 1/06 kann SMTP die TLS (Transport Layer Security) in Version 8.13 von sendmail verwenden, um dieses Problem zu beheben. Dieser erweiterte Service für SMTP-Server und -Clients bietet Folgendes:

- Private, authentifizierte Kommunikation über das Internet
- Schutz vor Lauschern und Angreifern

Hinweis – Die Implementierung von TLS basiert auf dem SSL-Protokoll (Secure Sockets Layer).

STARTTLS ist das SMTP-Schlüsselwort, das eine sichere SMTP-Verbindung mithilfe von TLS initiiert. Diese sichere Verbindung kann zwischen zwei Servern oder zwischen einem Server und einem Client hergestellt werden. Eine sichere Verbindung wird wie folgt definiert:

- Die E-Mail-Quelladresse und die Zieladresse sind verschlüsselt.
- Der Inhalt der E-Mail ist verschlüsselt.

Sobald der Client den Befehl STARTTLS ausgibt, antwortet der Server wie folgt:

- `220 Ready to start TLS`
- `501 Syntax error (no parameters allowed)`
- `454 TLS not available due to temporary reason`

Die Antwort 220 erfordert, dass der Client die TLS-Aushandlung startet. Die Antwort 501 weist darauf hin, dass der Client den Befehl STARTTLS falsch ausgegeben hat. STARTTLS wird ohne Parameter ausgegeben. Die Antwort 454 erfordert, dass der Client Regellistenwerte anwendet, um zu bestimmen, ob die Verbindung akzeptiert oder aufrechterhalten werden soll.

Beachten Sie, dass zur Aufrechterhaltung der SMTP-Infrastruktur des Internets öffentlich genutzte Server keine TLS-Aushandlung anfordern dürfen. Ein privat verwendeter Server kann jedoch den Client auffordern, eine TLS-Aushandlung durchzuführen. In solchen Fällen gibt der Server die folgende Antwort zurück:

```
530 Must issue a STARTTLS command first
```

Die Antwort 530 weist den Client an, den Befehl STARTTLS auszugeben, um eine Verbindung herzustellen.

Der Server oder Client kann eine Verbindung ablehnen, wenn der Grad der Authentifizierung und Vertraulichkeit nicht ausreicht. Da die meisten SMTP-Verbindungen nicht gesichert sind, ist es möglich, dass Server und Client eine nicht gesicherte Verbindung aufrechterhalten. Ob eine Verbindung aufrechterhalten oder abgelehnt wird, hängt von der Konfiguration des Servers und des Clients ab.

Die Unterstützung für die Ausführung von SMTP mit TLS ist nicht standardmäßig aktiviert. TLS wird aktiviert, wenn der SMTP-Client den Befehl STARTTLS ausgibt. Damit der SMTP-Client diesen Befehl ausgeben kann, müssen Sie die Zertifikate einrichten, die sendmail ermöglichen, TLS zu verwenden. Lesen Sie dazu „So richten Sie SMTP zur Verwendung von TLS ein“ auf Seite 317. Beachten Sie, dass dieses Verfahren das Definieren neuer Konfigurationsdateioptionen und das Neuerstellen Ihrer sendmail.cf-Datei umfasst.

Konfigurationsdateioptionen zum Ausführen von SMTP mit TLS

In der folgenden Tabelle werden die Konfigurationsdateioptionen beschrieben, die verwendet werden, um SMTP mit TLS auszuführen. Wenn Sie eine dieser Optionen deklarieren, verwenden Sie eine der folgenden Syntaxen:

- `O` *OptionName*= *argument* `# für die Konfigurationsdatei`
- `-O` *OptionName*= *argument* `# for the command line`
- `define('`*m4Name*`', `*argument*`) # für die m4-Konfiguration`

TABELLE 14–13 Konfigurationsdateioptionen zum Ausführen von SMTP mit TLS

Option	Beschreibung
`CACertFile`	`m4`-Name: `confCACERT`
	Argument: *filename*
	Standardwert: nicht definiert
	Kennzeichnet die Datei, die ein CA-Zertifikat enthält.
`CACertPath`	`m4`-Name: `confCACERT_PATH`
	Argument: *path*
	Standardwert: nicht definiert
	Kennzeichnet den Pfad zu dem Verzeichnis, das Zertifikate von CAs enthält.
`ClientCertFile`	`m4`-Name: `confCLIENT_CERT`
	Argument: *filename*
	Standardwert: nicht definiert
	Kennzeichnet die Datei, die das Zertifikat des Clients enthält. Beachten Sie, dass dieses Zertifikat verwendet wird, wenn `sendmail` als Client fungiert.
`ClientKeyFile`	`m4`-Name: `confCLIENT_KEY`
	Argument: *filename*
	Standardwert: nicht definiert
	Kennzeichnet die Datei, die den privaten Schlüssel enthält, der zum Clientzertifikat gehört.
`CRLFile`	`m4`-Name: `confCRL`
	Argument: *filename*
	Standardwert: nicht definiert
	Kennzeichnet die Datei, die den Zertifikat-Rücknahmestatus enthält, der für die X.509v3-Authentifizierung verwendet wird.

TABELLE 14–13 Konfigurationsdateioptionen zum Ausführen von SMTP mit TLS *(Fortsetzung)*

Option	Beschreibung
DHParameters	m4-Name: confDH_PARAMETERS Argument: *filename* Standardwert: nicht definiert Kennzeichnet die Datei, die die Diffie-Hellman-Parameter (DH) enthält.
RandFile	m4-Name: confRAND_FILE Argument: file:*filename* oder egd:*UNIX socket* Standardwert: nicht definiert Verwendet das file:-Präfix, um die Datei zu kennzeichnen, die Zufallsdaten enthält, oder verwendet das egd:-Präfix, um den UNIX-Socket zu kennzeichen. Beachten Sie, dass diese Option nicht festgelegt werden muss, da das Betriebssystem Solaris den Zufallszahlengenerator unterstützt. Weitere Informationen finden Sie auf der Manpage random(7D).
ServerCertFile	m4-Name: confSERVER_CERT Argument: *filename* Standardwert: nicht definiert Kennzeichnet die Datei, die das Zertifikat des Servers enthält. Dieses Zertifikat wird verwendet, wenn sendmail als Server fungiert.
Timeout.starttls	m4-Name: confTO_STARTTLS Argument: *amount of time* Standardwert: 1h Legt fest, wie lange der SMTP-Client auf die Antwort auf den Befehl STARTTLS wartet.
TLSSrvOptions	m4-Name: confTLS_SRV_OPTIONS Argument: V Standardwert: nicht definiert Legt fest, ob der Server ein Zertifikat vom Client verlangt. Wenn diese Option auf V gesetzt ist, wird keine Clientverifizierung durchgeführt.

Damit sendmail die SMTP-seitige Verwendung von TLS unterstützt, müssen folgende Optionen definiert sein:

- CACertPath
- CACertFile
- ServerCertFile
- ClientKeyFile

Andere Optionen sind nicht erforderlich.

Makros zum Ausführen von SMTP mit TLS

In der folgenden Tabelle werden die Makros beschrieben, die vom Befehl STARTTLS verwendet werden.

TABELLE 14–14 Makros zum Ausführen von SMTP mit TLS

Makro	Beschreibung
${cert_issuer}	Enthält den DN (Distinguished Name) der Zertifizierungsstelle (Certification Authority, CA), die das Zertifikat ausstellt.
${cert_subject}	Enthält den DN des Zertifikats, das als **cert subject** bezeichnet wird.
${cn_issuer}	Enthält den allgemeinen Namen (Common Name, CN) der Zertifizierungsstelle (CA), die das Zertifikat ausstellt (**cert issuer**).
${cn_subject}	Enthält den CN des Zertifikats, das als **cert subject** bezeichnet wird.
${tls_version}	Enthält die Version von TLS, die für die Verbindung verwendet wird.
${cipher}	Enthält eine Reihe von kryptografischen Algorithmen (**cipher suite**), die für die Verbindung verwendet werden.
${cipher_bits}	Enthält die Schlüssellänge des symmetrischen Verschlüsselungsalgorithmus (in Bits), der für die Verbindung verwendet wird.
${verify}	Enthält das Ergebnis der Verifizierung des vorgewiesenen Zertifikats. Folgende Werte sind möglich: ■ OK – Die Verifizierung wurde erfolgreich durchgeführt. ■ NO – Es wurde kein Zertifikat vorgewiesen. ■ NOT – Es wurde kein Zertifikat angefordert. ■ FAIL – Das vorgewiesene Zertifikat konnte nicht verifiziert werden. ■ NONE – STARTTLS wurde nicht ausgeführt. ■ TEMP – Ein zeitweiliger Fehler ist aufgetreten. ■ PROTOCOL – Ein SMTP-Fehler ist aufgetreten. ■ SOFTWARE – STARTTLS-Handshake ist fehlgeschlagen.
${server_name}	Enthält den Namen des Servers mit der aktuellen ausgehenden SMTP-Verbindung.
${server_addr}	Enthält die Adresse des Servers mit der aktuellen ausgehenden SMTP-Verbindung.

Regellisten zum Ausführen von SMTP mit TLS

In der folgenden Tabelle werden Regellisten beschrieben, die bestimmen, ob eine SMTP-Verbindung, die TLS verwendet, akzeptiert, gehalten oder abgelehnt wird.

TABELLE 14–15 Regellisten zum Ausführen von SMTP mit TLS

Regelliste	Beschreibung
tls_server	Wenn sendmail als Client fungiert, verwendet sendmail diese Regelliste, um zu festzustellen, ob der Server derzeit von TLS unterstützt wird.
tls_client	Wenn sendmail als Server fungiert, verwendet sendmail diese Regelliste, um zu festzustellen, ob der Client derzeit von TLS unterstützt wird.
tls_rcpt	Diese Regelliste erfordert eine Verifizierung des MTA des Empfängers. Diese empfängerbezogene Beschränkung macht Angriffe wie beispielsweise DNS-Spoofing unmöglich.
TLS_connection	Mit dieser Regelliste wird die Anforderung geprüft, die von RHS der Zugangs-Map für die Parameter der aktuellen TLS-Verbindung festgelegt wird.
try_tls	sendmail verwendet diese Regelliste, um die Ausführbarkeit von STARTTLS festzustellen, wenn eine Verbindung mit einem anderen MTA hergestellt wird. Wenn MTA den Befehl STARTTLS nicht richtig implementieren kann, wird STARTTLS nicht verwendet.

Weitere Informationen finden Sie unter http://www.sendmail.org/m4/starttls.html.

Sicherheitsüberlegungen zum Ausführen von SMTP mit TLS

SMTP ist ein Standard-Mailprotokoll, das Mailer definiert, die über das Internet ausgeführt werden, es ist jedoch kein Mechanismus zwischen Endgeräten. Aufgrund dieser Protokollbeschränkung gilt die Gewährleistung der TLS-Sicherheit auf Basis von SMTP für keine Mail-Benutzeragenten. Mail-Benutzeragenten dienen als Schnittstelle zwischen Benutzern und einem Mail Transfer Agent wie beispielsweise sendmail .

Mails können auch über mehrere Server weitergeleitet werden. Zur Gewährleistung einer umfassenden SMTP-Sicherheit muss TLS in der gesamten Kette der SMTP-Verbindungen unterstützt werden.

Außerdem muss der Grad der ausgehandelten Authentifizierung und Vertraulichkeit zwischen jedem Serverpaar oder zwischen einem Client und einem Server berücksichtigt werden. Weitere Informationen finden Sie unter „Authentifizierungsservices“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Zusätzliche Befehlszeilenoptionen in Version 8.13 von sendmail

In der folgenden Tabelle werden zusätzliche Befehlszeilenoptionen beschrieben, die in Version 8.13 von sendmail zur Verfügung stehen. Weitere Befehlszeilenoptionen sind auf der Manpage sendmail(1M) beschrieben.

TABELLE 14–16 Befehlszeilenoptionen in Version 8.13 von sendmail

Option	Beschreibung
-D *logfile*	Sendet eine Fehlersuchausgabe an die angegebene *logfile*, anstatt diese Informationen in die Standardausgabe einzubeziehen.
-q[!]Q*substr*	Legt die Verarbeitung von Jobs fest, die unter Quarantäne gestellt sind und die Unterzeichenfolge *substr* aufweisen (eine Unterzeichenfolge der Quarantäneursache *reason*). Weitere Informationen finden Sie in der Beschreibung der Option -Q*reason*. Wenn ! hinzugefügt wird, werden mit dieser Option die unter Quarantäne gestellten Jobs verarbeitet, die die Unterzeichenfolge (*substr*) nicht aufweisen.
-Q*reason*	Stellt ein normales Warteschlangenelement mit dieser Ursache (*reason*) unter Quarantäne. Wenn keine Ursache (*reason*) angegeben ist, wird die Quarantäne des unter Quarantäne gestellte Warteschlangenelements aufgehoben. Diese Option kann zusammen mit der Option -q[!]Q*substr* verwendet werden. *substr* ist ein Teil (bzw. Unterzeichenfolge) von *reason*.

Zusätzliche und überarbeitete Konfigurationsdateioptionen in Version 8.13 von sendmail

In der folgenden Tabelle werden die zusätzlichen und überarbeiteten Konfigurationsdateioptionen beschrieben. Wenn Sie eine dieser Optionen deklarieren, verwenden Sie eine der folgenden Syntaxen:

```
O OptionName=argument          # for the configuration file
-O OptionName=argument         # for the command line
define(‘m4Name’,argument)     # for m4 configuration
```

TABELLE 14–17 Konfigurationsdateioptionen in Version 8.13 von sendmail

Option	Beschreibung
ConnectionRateWindowSize	m4-Name: confCONNECTION_RATE_WINDOW_SIZE Argument: *Zahl* Standardwert: 60 Legt die Anzahl von Sekunden für die Haltezeit von eingehenden Verbindungen fest.
FallBackSmartHost	m4-Name: confFALLBACK_SMARTHOST Argument: *hostname* Verwenden Sie diese Option, um einen gut verbundenen Host zu gewährleisten, der als Backup oder Failover für alle fehlgeschlagenen MX-Datensätze dient, und um sicherzustellen, dass die Mails an die Clients übermittelt werden.

TABELLE 14–17 Konfigurationsdateioptionen in Version 8.13 von sendmail *(Fortsetzung)*

Option	Beschreibung
InputMailFilters	m4-Name: confINPUT_MAIL_FILTERS Argument: *filename* Listet die Eingangsmailfilter für den sendmail-Dämon auf.
PidFile	m4Name: confPID_FILE Argument: *filename* Standardwert: /var/run/sendmail.pid Der Dateiname wird wie in früheren Versionen durch ein Makro erweitert, bevor er geöffnet wird. In Version 8.13 wird zudem die Verknüpfung der Datei aufgehoben, wenn sendmail vorhanden ist.
QueueSortOrder	m4-Name: confQUEUE_SORT_ORDER Hinzugefügtes Argument: none In Version 8.13 wird none verwendet, um anzugeben, das keine Sortierreihenfolge verwendet wird.
RejectLogInterval	m4-Name: confREJECT_LOG_INTERVAL Argument: *period-of-time* Standardwert: 3h (drei Stunden) Wenn eine Dämonverbindung aufgrund der angegebenen Dauer (*period-of-time*) abgelehnt wird, werden die betreffenden Informationen protokolliert.
SuperSafe	m4-Name: confSAFE_QUEUE Kurzname: s Hinzugefügtes Argument: postmilter Standardwert: true Wenn postmilter gesetzt ist, setzt sendmail die Synchronisierung der Warteschlangendatei aus, bis alle milters signalisiert haben, dass die Nachricht akzeptiert wurde. Um dieses Argument zu verwenden, muss sendmail als SMTP-Server ausgeführt werden. Anderenfalls funktioniert postmilter in gleicher Weise wie das Argument true.

Zusätzliche und überarbeitete FEATURE()-Deklarationen in Version 8.13 von sendmail

In der folgenden Tabelle werden die zusätzlichen und überarbeiteten FEATURE()-Deklarationen beschrieben. Dieses m4-Makro verwendet die folgende Syntax:

```
FEATURE(‘name’, ‘argument’)
```

TABELLE 14–18 FEATURE()-Deklarationen in Version 8.13 von sendmail

Name von FEATURE()	Beschreibung
conncontrol	Wird in Verbindung mit der access_db-Regelliste verwendet, um die Anzahl der eingehenden SMTP-Verbindungen zu prüfen. Weitere Informationen finden Sie in der Datei /etc/mail/cf/README.
greet_pause	Fügt die greet_pause-Regelliste hinzu, die Open-Proxy- and SMTP-Slamming-Schutz ermöglicht. Weitere Informationen finden Sie in der Datei /etc/mail/cf/README .
local_lmtp	Das Standardargument ist weiterhin mail.local, der LMTP-fähige Mailer in dieser Solaris-Version. Wird in Version 8.13 jedoch ein anderer LMTP-fähiger Mailer verwendet, kann dessen Pfadname als zweiter Parameter angegeben werden, und die Argumente, die an den zweiten Parameter weitergegeben werden, können im dritten Parameter angegeben werden. Beispiel: FEATURE(‘local_lmtp’, ‘/usr/local/bin/lmtp’, ‘lmtp’)
mtamark	Bietet experimentelle Unterstützung für "Marking Mail Transfer Agents in Reverse DNS with TXT RRs" (MTAMark) . Weitere Informationen finden Sie in der Datei /etc/mail/cf/README .
ratecontrol	Arbeitet in Verbindung mit der access_db-Regelliste, um Verbindungsraten für Hosts zu steuern. Weitere Informationen finden Sie in der Datei /etc/mail/cf/README .
use_client_ptr	Wenn dieses FEATURE() aktiviert ist, setzt die Regelliste check_relay ihr erstes Argument mit diesem Argument, $&{client_ptr} , außer Kraft.

Änderungen ab Version 8.12 von sendmail

Dieser Abschnitt enthält Informationen über folgende Themen:

- „Unterstützung für TCP-Wrapper ab Version 8.12 von sendmail“ auf Seite 401
- „submit.cf-Konfigurationsdatei der Version 8.12 von sendmail“ auf Seite 401
- „Zusätzliche oder eingestellte Befehlszeilenoptionen ab Version 8.12 von sendmail“ auf Seite 403
- „Zusätzliche Argumente für die Optionen PidFile und ProcessTitlePrefix ab Version 8.12 von sendmail“ auf Seite 404
- „Zusätzliche definierte Makros ab Version 8.12 von sendmail“ auf Seite 405
- „Zusätzliche Makros ab Version 8.12 von sendmail“ auf Seite 406
- „Zusätzliche MAX-Macros ab Version 8.12 von sendmail“ auf Seite 407
- „Zusätzliche und überarbeitete m4-Konfigurationsmakros ab Version 8.12 von sendmail“ auf Seite 408
- „Änderungen an der FEATURE()-Deklaration ab Version 8.12 von sendmail“ auf Seite 408
- „Änderungen an der MAILER()-Deklaration ab Version 8.12 von sendmail“ auf Seite 411
- „Zusätzliche Delivery Agents-Flags ab Version 8.12 von sendmail“ auf Seite 412
- „Zusätzliche Gleichsetzungen für Delivery Agents ab Version 8.12 von sendmail“ auf Seite 412
- „Zusätzliche Warteschlangenfunktionen ab Version 8.12 von sendmail“ auf Seite 414

- „Änderungen für LDAP ab Version 8.12 von sendmail “ auf Seite 414
- „Änderung am integrierten Mailer ab Version 8.12 von sendmail“ auf Seite 416
- „Zusätzliche Regellisten ab Version 8.12 von sendmail“ auf Seite 416
- „Änderungen an Dateien ab Version 8.12 von sendmail “ auf Seite 417
- „sendmail-Version 8.12 und IPv6-Adressen in der Konfiguration“ auf Seite 418

Unterstützung für TCP-Wrapper ab Version 8.12 von sendmail

TCP-Wrapper dienen zur Implementierung der Zugriffskontrollen. Dazu wird die Adresse eines Hosts, der einen bestimmten Netzwerkdienst anfordert, anhand einer Zugriffskontrollliste (Access Control List, ACL) geprüft. Anforderungen werden dann entsprechend genehmigt oder verweigert. Zusätzlich zur Bereitstellung dieses Zugriffkontrollmechanismus protokollieren die TCP-Wrapper auch Hostanforderungen für Netzwerkdienste und führen somit eine wichtige Überwachungsfunktion aus. Beispiele für Netzwerkdienste, die dieser Zugriffskontrolle unterzogen werden, sind `rlogind`, `telnetd` und `ftpd`.

Ab Version 8.12 ermöglicht `sendmail` die Verwendung von TCP-Wrappern. Diese Prüfung umgeht jedoch keine anderen Sicherheitsmaßnahmen. Durch das Aktivieren von TCP-Wrappern in `sendmail` wird eine Prüfung hinzugefügt, um die Quelle von Netzwerkanforderungen zu validieren, bevor die Anforderung genehmigt wird. Weitere Informationen finden Sie auf der Manpage `hosts_access`(4).

Hinweis – Unterstützung für TCP-Wrapper in `inetd`(1M) und `sshd`(1M) ist ab Solaris 9 verfügbar.

Informationen zu Zugriffskontrolllisten finden Sie unter „Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

`submit.cf`-Konfigurationsdatei der Version 8.12 von `sendmail`

Ab Version 8.12 enthält `sendmail` eine zusätzliche Konfigurationsdatei, `/etc/mail/submit.cf`. Diese Datei, `submit.cf`, wird verwendet, um `sendmail` im Modus des Mailübergabeprogramms anstelle des Dämonmodus auszuführen. Im Gegensatz zum Dämonmodus benötigt der Modus des Mailübergabeprogramms keine `root`-Berechtigung. Dieses neue Paradigma bietet daher mehr Sicherheit.

In der nachstehenden Liste werden die Funktionen von submit.cf beschrieben:

- sendmail verwendet submit.cf für die Ausführung im Modus des Mail-Übergabeprogramms (Mail-Submission Program, MSP). Dieser Modus dient zur Übergabe von E-Mails und kann durch Programme (z. B. mailx) und Benutzer gestartet werden kann. Weitere Informationen finden Sie in den Beschreibungen der Optionen -Ac und -Am auf der Manpage sendmail(1M).
- submit.cf wird in den folgenden Betriebsmodi verwendet:
  - -bm – der Standard-Betriebsmodus
  - -bs – ein Betriebsmodus, in dem die Standardeingabe verwendet wird, um SMTP auszuführen
  - -bt – ein Testmodus zum Auflösen von Adressen
- sendmail wird nicht als SMTP-Dämon ausgeführt, wenn die Datei submit.cf verwendet wird.
- Wenn sendmail die Datei submit.cf verwendet, wird die ausschließlich für Clients reservierte Warteschlange (/var/spool/clientmqueue) verwendet, in der Nachrichten enthalten sind, die nicht an den sendmail-Dämon übermittelt wurden. Die Nachrichten in der ausschließlich für Clients reservierten Warteschlange werden durch den Clientdämon übermittelt, der als Clientwarteschlangen-Betriebsprogramm fungiert.
- sendmail verwendet standardmäßig submit.cf in regelmäßigen Abständen, um die MSP-Warteschlange, /var/spool/clientmqueue, auszuführen.

  ```
  /usr/lib/sendmail -Ac -q15m
  ```

Beachten Sie Folgendes:

- Ab Solaris 9 wird submit.cf automatisch bereitgestellt.
- submit.cf erfordert keine Planung oder vorläufigen Verfahren, die vor der Installation von Solaris 9 oder einer neueren Version ausgeführt werden müssen.
- sendmail verwendet automatisch submit.cf, sofern Sie keine Konfigurationsdatei angeben. sendmail kennt sowohl die Aufgaben für submit.cf als auch die Aufgaben für sendmail.cf.

Funktionen, die sendmail.cf von submit.cf unterscheiden

Die sendmail.cf-Konfigurationsdatei ist für den Dämonmodus vorgesehen. Wenn diese Datei verwendet wird, fungiert sendmail als MTA (Mail Transfer Agent), der von root gestartet wird.

```
/usr/lib/sendmail -L sm-mta -bd -q1h
```

In der nachstehenden Liste finden Sie weitere unterscheidende Funktionen für sendmail.cf :

- SMTP-Verbindungen an den Ports 25 und 587 werden von sendmail.cf standardmäßig akzeptiert.
- sendmail.cf führt standardmäßig die Hauptwarteschlange (/var/spool/mqueue) aus.

Funktionelle Änderungen ab Version 8.12 von sendmail

Mit submit.cf gehen folgende funktionelle Änderungen einher:

- Ab Version 8.12 von sendmail kann die Mailwarteschlange nur vom root-Benutzer ausgeführt werden. Weitere Informationen finden Sie in den Beschreibungen der Änderungen auf der Manpage mailq(1). Neue aufgabenbezogene Informationen finden Sie unter „Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)“ auf Seite 336.
- Der Modus des Mailübergabeprogramms wird ohne root-Berechtigung ausgeführt. Aus diesem Grund kann sendmail möglicherweise auf bestimmte Dateien (z. B. .forward-Dateien) nicht zugreifen. Die Option -bv von sendmail könnte folglich eine für den Benutzer irreführende Ausgabe erzeugen. Eine Problemumgehung ist nicht verfügbar.
- Wenn Sie vor Version 8.12 sendmail nicht im Dämonmodus ausgeführt haben, wurde nur die Übermittlung von eingehenden Mails verhindert. Ab Version 8.12 von sendmail verhindern Sie jedoch auch die Übermittlung von abgehenden Mails, wenn Sie den sendmail-Dämon nicht mit der Standardkonfiguration ausführen. Das Clientwarteschlangen-Betriebsprogramm (auch Mailübergabeprogramm genannt) muss Mails an den Dämon am lokalen SMTP-Port senden können. Wenn das Clientwarteschlangen-Betriebsprogramm versucht, eine SMTP-Sitzung mit dem lokalen Host zu starten, und der Dämon den SMTP-Port nicht überwacht, bleiben die Mails in der Warteschlange. Bei der Standardkonfiguration wird ein Dämon ausgeführt. Dieses Problem tritt folglich nicht auf, wenn Sie die Standardkonfiguration verwenden. Wenn Sie jedoch Ihren Dämon deaktiviert haben, finden Sie unter „So verwalten Sie die Mailübermittlung mithilfe einer alternativen Konfiguration von sendmail.cf“ auf Seite 322 eine Anleitung, um dieses Problem zu beheben.

Zusätzliche oder eingestellte Befehlszeilenoptionen ab Version 8.12 von sendmail

In der folgenden Tabelle werden zusätzliche oder eingestellte Befehlszeilenoptionen für sendmail beschrieben. Weitere Befehlszeilenoptionen sind auf der Manpage sendmail(1M) beschrieben.

TABELLE 14–19 Zusätzliche oder eingestellte Befehlszeilenoptionen ab Version 8.12 von sendmail

Option	Beschreibung
-Ac	Zeigt an, dass die Konfigurationsdatei submit.cf auch dann verwendet werden soll, wenn der Betriebsmodus keine erstmalige Mailübergabe anzeigt. Weitere Informationen zu submit.cf finden Sie unter „submit.cf-Konfigurationsdatei der Version 8.12 von sendmail“ auf Seite 401.
-Am	Zeigt an, dass die Konfigurationsdatei sendmail.cf auch dann verwendet werden soll, wenn der Betriebsmodus eine anfängliche Mailübergabe anzeigt. Weitere Informationen finden Sie unter „submit.cf-Konfigurationsdatei der Version 8.12 von sendmail“ auf Seite 401.

TABELLE 14–19 Zusätzliche oder eingestellte Befehlszeilenoptionen ab Version 8.12 von sendmail *(Fortsetzung)*

Option	Beschreibung
-bP	Zeigt an, dass Sie die Anzahl der Einträge in jeder Warteschlange ausgeben.
-G	Zeigt an, dass die über die Befehlszeile weitergeleitete Nachricht für die Weiterleitung bestimmt ist, nicht für die anfängliche Übergabe. Die Nachricht wird zurückgewiesen, wenn die Adressen nicht voll qualifiziert sind. Es wird keine Kanonisierung durchgeführt. Wie in den Versionshinweisen erwähnt, die Teil der sendmail-Distribution auf ftp://ftp.sendmail.org sind, werden falsch gebildete Nachrichten in neueren Versionen u. U. abgelehnt.
-L *tag*	Setzt die ID, die für syslog-Nachrichten verwendet wird, auf das angegebene *tag*.
-q[!]I *substring*	Verarbeitet nur Jobs, die die Unterzeichenfolge (*substring*) eines der Empfänger aufweisen. Wenn ! hinzugefügt wird, werden mit dieser Option nur Jobs verarbeitet, die diesen *substring* nicht enthalten.
-q[!]R *substring*	Verarbeitet nur Jobs, die die Unterzeichenfolge (*substring*) der Warteschlangen-ID aufweisen. Wenn ! hinzugefügt wird, werden mit dieser Option nur Jobs verarbeitet, die diesen *substring* der Warteschlangen-ID nicht enthalten.
-q[!]S *substring*	Verarbeitet nur Jobs, die die Unterzeichenfolge (*substring*) des Absenders aufweisen. Wenn ! hinzugefügt wird, werden mit dieser Option nur Jobs verarbeitet, die diesen *substring* des Absenders nicht enthalten.
-qf	Verarbeitet gespeicherte Nachrichten in der Warteschlange ein Mal, ohne den fork -Systemaufruf zu verwenden, und führt den Vorgang im Vordergrund aus. Weitere Informationen finden Sie auf der Manpage fork(2).
-qG*name*	Verarbeitet nur die Nachrichten in der *name*-Warteschlangengruppe.
-qp*time*	Verarbeitet in der Warteschlange gespeicherte Nachrichten in bestimmten Zeitintervallen, wobei ein einzelner untergeordneter Prozess ausgeführt wird, der für jede Warteschlange verzweigt wird. Der untergeordnete Prozess ist zwischen den Warteschlangenprozessintervallen inaktiv. Diese neue Option ist der Option -q*time* ähnlich, die periodisch einen untergeordneten Prozess verwendet, um die Warteschlange zu verarbeiten.
-U	Wie in den Versionshinweisen erwähnt, die Teil der sendmail-Distribution auf ftp://ftp.sendmail.org sind, steht diese Option ab der Version 8.12 nicht mehr zur Verfügung. Mail-Benutzeragenten sollten das Argument -G verwenden.

Zusätzliche Argumente für die Optionen PidFile und ProcessTitlePrefix ab Version 8.12 von sendmail

In der folgenden Tabelle werden zusätzliche, mithilfe von Makros verarbeitete Argumente für die Optionen PidFile und ProcessTitlePrefix beschrieben. Weitere Informationen zu diesen Optionen finden Sie auf der Manpage sendmail(1M).

TABELLE 14–20 Argumente für die Optionen PidFile und ProcessTitlePrefix

Makro	Beschreibung
${daemon_addr}	Bereitstellung der Dämonadresse (beispielsweise 0.0.0.0)
${daemon_family}	Bereitstellung der Dämonfamilie (z. B. inet und inet6)
${daemon_info}	Bereitstellung von Dämoninformationen (z. B. SMTP+queueing@00:30:00)
${daemon_name}	Bereitstellung des Dämonnamens (z. B. MSA)
${daemon_port}	Bereitstellung des Dämonports (z. B. 25)
${queue_interval}	Bereitstellung des Warteschlangenbetriebsintervalls (z. B. 00:30:00)

Zusätzliche definierte Makros ab Version 8.12 von sendmail

In der folgenden Tabelle werden zusätzliche Makros beschrieben, die für das sendmail -Programm reserviert sind. Die Werte der Makros werden intern zugewiesen. Weitere Informationen finden Sie auf der Manpage sendmail(1M).

TABELLE 14–21 Zusätzliche definierte Makros für sendmail

Makro	Beschreibung
${addr_type}	Erkennt die aktuelle Adresse als Absender- oder Empfängeradresse.
${client_resolve}	Enthält das Ergebnis des Auflösungsaufrufs für ${client_name}: OK, FAIL, FORGED oder TEMP.
${deliveryMode}	Gibt den aktuellen Übermittlungsmodus an, den sendmail anstelle des Werts der DeliveryMode-Option verwendet.
${dsn_notify}, ${dsn_envid}, ${dsn_ret}	Enthält die entsprechenden DSN-Parameterwerte.
${if_addr}	Stellt die Schnittstellenadresse für die eingehende Verbindung bereit, wenn die Schnittstelle nicht zum Loopback-Netzwerk gehört. Dieses Makro eignet sich insbesondere für virtuelles Hosting.

TABELLE 14–21 Zusätzliche definierte Makros für sendmail *(Fortsetzung)*

Makro	Beschreibung
${if_addr_out}, ${if_name_out}, ${if_family_out}	Vermeidet die wiederholte Verwendung von ${if_addr}. Enthält folgende Werte: Adresse der Schnittstelle für die abgehende Verbindung Hostname der Schnittstelle für die abgehende Verbindung Familie der Schnittstelle für die abgehende Verbindung
${if_name}	Stell den Hostnamen der Schnittstelle für die eingehende Verbindung bereit und ist insbesondere für virtuelles Hosting geeignet.
${load_avg}	Prüft und meldet die aktuelle durchschnittliche Anzahl von Jobs in der Ausführungswarteschlange.
${msg_size}	Enthält den Wert der Nachrichtengröße (SIZE=parameter) in einem ESMTP-Dialog, bevor die Nachricht erfasst wird. Danach enthält das Makro die Nachrichtengröße, wie sie von sendmail errechnet wurde. Sie wird in check_compat verwendet. Weitere Informationen zu check_compat finden Sie in Tabelle 14–25.
${nrcpts}	Enthält die Anzahl der validierten Empfänger.
${ntries}	Enthält die Anzahl der Übermittlungsversuche.
${rcpt_mailer}, ${rcpt_host}, ${rcpt_addr}, ${mail_mailer}, ${mail_host}, ${mail_addr}	Enthält die Ergebnisse der Analyse der Argumente RCPT und MAIL. Hierbei handelt es sich um die drei aufgelösten Elemente, die rechts neben dem Mail Delivery Agent ($#*mailer*), dem Host ($@*host*) und dem Benutzer ($:*addr*) stehen.

Zusätzliche Makros ab Version 8.12 von sendmail

Dieser Abschnitt enthält eine Tabelle, in der die zusätzlichen Makros beschrieben sind, die verwendet werden, um die sendmail-Konfigurationsdatei zu erstellen.

TABELLE 14–22 Zusätzliche Makros zum Erstellen der sendmail-Konfigurationsdatei

Makro	Beschreibung
LOCAL_MAILER_EOL	Setzt die standardmäßige Zeilenenden-Zeichenfolge für den lokalen Mailer außer Kraft.

TABELLE 14–22 Zusätzliche Makros zum Erstellen der sendmail-Konfigurationsdatei *(Fortsetzung)*

Makro	Beschreibung
LOCAL_MAILER_FLAGS	Fügt standardmäßig die Return-Path:-Kopfzeile hinzu.
MAIL_SETTINGS_DIR	Enthält den Pfad (einschließlich des nachstehenden Schrägstrichs) des Verzeichnisses der Maileinstellungen.
MODIFY_MAILER_FLAGS	Verbessert die *_MAILER_FLAGS. Dieses Makro dient zum Festlegen, Hinzufügen und Löschen von Flags.
RELAY_MAILER_FLAGS	Definiert zusätzliche Flags für den Relay Mailer.

Zusätzliche MAX-Macros ab Version 8.12 von sendmail

Verwenden Sie die folgenden Makros, um die maximale Anzahl von Befehlen zu konfigurieren, die empfangen werden können, bevor sendmail die Übermittlung verlangsamt. Sie können diese MAX-Makros während der Kompilierung festlegen. Die in der folgenden Tabelle angegebenen maximalen Werte sind zugleich die aktuellen Standardwerte.

TABELLE 14–23 Zusätzliche MAX-Makros

Makro	Höchstwert	Befehle, die von jedem Makro geprüft werden
MAXBADCOMMANDS	25	Unbekannte Befehle
MAXNOOPCOMMANDS	20	NOOP, VERB, ONEX, XUSR
MAXHELOCOMMANDS	3	HELO, EHLO
MAXVRFYCOMMANDS	6	VRFY, EXPN
MAXETRNCOMMANDS	8	ETRN

Hinweis – Sie können die Prüfung eines Makros deaktivieren, indem Sie den Wert des Makros auf null setzen.

Zusätzliche und überarbeitete m4-Konfigurationsmakros ab Version 8.12 von sendmail

Dieser Abschnitt enthält eine Tabelle mit zusätzlichen und überarbeiteten m4-Konfigurationsmakros für sendmail. Verwenden Sie die folgende Syntax, um diese Makros zu deklarieren:

symbolic-name(‘*value*’)

Informationen zum Erstellen einer neuen sendmail.cf-Datei finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“.

TABELLE 14–24 Zusätzliche und überarbeitete m4-Konfigurationsmakros für sendmail

m4-Makro	Beschreibung
FEATURE()	Ausführliche Informationen finden Sie unter „Änderungen an der FEATURE()-Deklaration ab Version 8.12 von sendmail“ auf Seite 408.
LOCAL_DOMAIN()	Dieses Makro fügt der Klasse w ($=w) Einträge hinzu.
MASQUERADE_EXCEPTION()	Ein neues Makro, das Hosts oder Teildomains definiert, die nicht maskiert werden können.
SMART_HOST()	Dieses Makro kann jetzt für Adressen verwendet werden, die in eckigen Klammern stehen, z. B. user@[*host*].
VIRTUSER_DOMAIN() oder VIRTUSER_DOMAIN_FILE()	Wenn diese Makros verwendet werden, fügen Sie $={VirtHost} in $=R ein. Hinweis: $=R sind die Namen der Hosts, die eine Weiterleitung durchführen können.

Änderungen an der FEATURE()-Deklaration ab Version 8.12 von sendmail

In der folgenden Tabelle finden Sie Informationen zu den jeweiligen Änderungen an den FEATURE()-Deklarationen.

Um die neuen und überarbeiteten FEATURE-Namen zu nutzen zu können, verwenden Sie die folgende Syntax:

FEATURE(‘*name*’, ‘*argument*’)

Informationen zum Erstellen einer neuen sendmail.cf-Datei finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“.

TABELLE 14–25 Zusätzliche und überarbeitete FEATURE()-Deklarationen

Name von FEATURE()	Beschreibung
compat_check	Argument: Siehe Beispiel im folgenden Abschnitt. Dieses neue FEATURE() ermöglicht Ihnen, nach einem Schlüssel in der Zugriffs-Map zu suchen, der aus der Absenderadresse und der Empfängeradresse besteht. Dieses FEATURE() wird durch die Zeichenfolge <@> getrennt. Beispiel: *sender*@*sdomain*<@>*recipient* @*rdomain*.
delay_checks	Argument: friend, das einen Spam-Friend-Test aktiviert, oder hater, das einen Spam-Hater-Test aktiviert. Ein neues FEATURE(), das alle Prüfungen verzögert. Wird FEATURE('delay_checks') verwendet, werden die Regellisten check_mail und check_relay nicht aufgerufen, wenn ein Client eine Verbindung mit einem MAIL-Befehl herstellt bzw. einen solchen Befehl ausgibt. Stattdessen werden diese Regellisten durch die Regelliste check_rcpt aufgerufen. Ausführliche Informationen finden Sie in der Datei /etc/mail/cf/README.
dnsbl	Argument: Dieses FEATURE() akzeptiert maximal zwei Argumente: ■ DNS-Servername ■ Ablehnungsnachricht Ein neues FEATURE(), das Sie mehrmals verwenden können, um die Rückgabewerte für DNS-Suchvorgänge zu prüfen. Dieses FEATURE() ermöglicht Ihnen, das Verhalten von zeitweilig fehlgeschlagenen Suchvorgängen anzugeben.
enhdnsbl	Argument: Domainname Ein neues FEATURE(), das eine verbesserte Version von dnsbl ist. Damit können Sie die Rückgabewerte für DNS-Suchvorgänge prüfen. Weitere Informationen finden Sie in der Datei /etc/mail/cf/README.
generics_entire_domain	Argument: keines Eine neues FEATURE(), das Sie auch verwenden können, um genericstable für Teildomains von $=G zu übernehmen.
ldap_routing	Argument: Weitere Informationen finden Sie in den Versionshinweisen unter http://www.sendmail.org. Ein neues FEATURE(), das das LDAP-Adressen-Routing implementiert.
local_lmtp	Argument: Pfadname eines LMTP-fähigen Mailers. Der LMTP-fähige Standardmailer in dieser Solaris-Version ist mail.local. Ein FEATURE(), das jetzt den DSN-Diagnosecodetyp für den lokalen Mailer auf den entsprechenden Wert von SMTP setzt.
local_no_masquerade	Argument: keines Ein neues FEATURE(), das Sie verwenden können, um die Maskierung des lokalen Mailers zu vermeiden.

TABELLE 14–25 Zusätzliche und überarbeitete FEATURE()-Deklarationen *(Fortsetzung)*

Name von FEATURE()	Beschreibung
lookupdotdomain	Argument: keines Ein neues FEATURE(), das Sie verwenden können, um nach der *.domain* in der Zugriffs-Map zu suchen.
nocanonify	Argument: canonify_hosts oder keines Ein FEATURE(), das jetzt folgende Funktionen bietet: Ermöglicht die Weitergabe einer Liste von Domains entsprechend den Angaben von CANONIFY_DOMAIN oder CANONIFY_DOMAIN_FILE an die Operatoren $[und $] für die Kanonisierung. Ermöglicht die Kanonisierung von Adressen, die nur einen Hostnamen haben, wie beispielsweise <user@host> , wenn canonify_hosts als Parameter festgelegt ist. Fügt einen nachgestellten Punkt in Adressen ein, die aus mehreren Komponenten bestehen.
no_default_msa	Argument: keines Ein neues FEATURE(), das die Standardeinstellung von sendmail in den m4-generierten Konfigurationsdateien zum Überwachen verschiedener Ports deaktiviert – eine Implementierung von RFC 2476.
nouucp	Argument: reject, wodurch das Token ! nicht zugelassen wird, oder nospecial, wodurch das Token ! zugelassen wird. Ein FEATURE(), das festlegt, ob das Token ! im lokalen Teil einer Adresse zugelassen wird.
nullclient	Argument: keines Ein FEATURE(), das jetzt die vollständige Regelliste einer normalen Konfiguration bereitstellt und so die Durchführung von Antispam-Prüfungen zulässt.
preserve_local_plus_detail	Argument: keines Ein neues FEATURE(), das Ihnen ermöglicht, den +detail-Teil der Adresse zu erhalten, wenn sendmail die Adresse an den lokalen Delivery Agent weiterleitet.
preserve_luser_host	Argument: keines Ein neues FEATURE(), das Ihnen ermöglicht, den Namen des empfangenden Hosts zu erhalten, wenn LUSER_RELAY verwendet wird.
queuegroup	Argument: keines Ein neues FEATURE(), das Ihnen ermöglicht, eine Gruppe von Warteschlangen auszuwählen, die auf der vollständigen E-Mail-Adresse oder der Domain des Empfängers basiert.

TABELLE 14–25 Zusätzliche und überarbeitete FEATURE()-Deklarationen *(Fortsetzung)*

Name von FEATURE()	Beschreibung
relay_mail_from	Argument: Die Domain (*domain*) ist ein optionales Argument. Ein neues FEATURE(), das die Weiterleitung ermöglicht, wenn der Absender der Mail in der Zugriffs-Map als RELAY aufgelistet ist und durch die Kopfzeile Von: gekennzeichnet ist. Wenn das optionale Argument *domain* angegeben ist, wird auch der Domainteil des Absenders der Mail geprüft.
virtuser_entire_domain	Argument: keines Ein FEATURE(), mit dem Sie jetzt die Klasse $={VirtHost} anwenden können. Diese neue Klasse dient zum Abgleichen von virtusertable-Einträgen, die durch VIRTUSER_DOMAIN oder VIRTUSER_DOMAIN_FILE gefüllt werden können. FEATURE(‘virtuser_entire_domain’) kann die Klasse $={VirtHost} auch auf ganze Teildomains anwenden.

Die folgenden FEATURE()-Deklarationen werden nicht mehr unterstützt.

TABELLE 14–26 Nicht unterstützte FEATURE()-Deklarationen

Name von FEATURE()	Ersatz
rbl	FEATURE(‘dnsbl’) und FEATURE(‘enhdnsbl’) ersetzen das entfernte FEATURE().
remote_mode	MASQUERADE_AS(‘$S’) ersetzt FEATURE(‘remote_mode’) in /etc/mail/cf/subsidiary.mc. $S ist der SMART_HOST-Wert in sendmail.cf.
sun_reverse_alias_files	FEATURE(‘genericstable’)
sun_reverse_alias_nis	FEATURE(‘genericstable’)
sun_reverse_alias_nisplus	FEATURE(‘genericstable’)

Änderungen an der MAILER()-Deklaration ab Version 8.12 von sendmail

Die MAILER()-Deklaration definiert die Unterstützung von Delivery Agents. Um einen Delivery Agent zu deklarieren, verwenden Sie die folgende Syntax:

MAILER(‘*symbolic-name*’)

Beachten Sie die folgenden Änderungen:

- In dieser neuen Version von sendmail enthält die MAILER(‘smtp’)-Deklaration einen zusätzlichen Mailer, dsmtp, der mithilfe des Mailer-Flag F=% für eine bedarfsorientierte Übermittlung sorgt. Die dsmtp-Mailer-Definition verwendet das neue DSMTP_MAILER_ARGS, das standardmäßig auf IPC $h gesetzt wird.

- Zahlen für Regellisten, die von MAILERn verwendet werden, wurden entfernt. MAILER müssen jetzt nicht mehr in einer bestimmten Reihenfolge aufgelistet werden, ausgenommen MAILER('uucp'), der hinter MAILER('smtp') stehen muss, wenn uucp-dom und uucp-uudom verwendet werden.

Weitere Informationen zu Mailern finden Sie unter „Mailer und sendmail“ auf Seite 356. Informationen zum Erstellen einer neuen sendmail.cf-Datei finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“.

Zusätzliche Delivery Agents-Flags ab Version 8.12 von sendmail

In der folgenden Tabelle werden zusätzliche Flags für Delivery Agents beschrieben, die nicht standardmäßig festgelegt sind. Diese aus einem Zeichen bestehenden Flags sind boolesche Werte. Sie können ein Flag setzen oder zurücksetzen, indem Sie es in die F=-Anweisung Ihrer Konfigurationsdatei einschließen oder aus dieser ausschließen (siehe folgendes Beispiel).

```
Mlocal,     P=/usr/lib/mail.local, F=lsDFMAw5:/|@qSXfmnz9, S=10/30, R=20/40,
Mprog,      P=/bin/sh, F=lsDFMoqeu9, S=10/30, R=20/40, D=$z:/,
Msmtp,      P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,
Mesmtp,     P=[IPC], F=mDFMuXa, S=11/31, R=21, E=\r\n, L=990,
Msmtp8,     P=[IPC], F=mDFMuX8, S=11/31, R=21, E=\r\n, L=990,
Mrelay,     P=[IPC], F=mDFMuXa8, S=11/31, R=61, E=\r\n, L=2040,
```

TABELLE 14–27 Zusätzliche Mailer-Flags

Flag	Beschreibung
%	Mailer, die dieses Flag verwenden, versuchen nur dann, eine Nachricht an den anfänglichen Empfänger oder an die Warteschlangenprozesse weiterzuleiten, wenn die Nachricht in der Warteschlange mithilfe der ETRN-Anfrage oder einer der folgenden Warteschlangenoptionen ausgewählt wird: -qI, -qR oder -qS.
1	Dieses Flag deaktiviert die Funktion des Mailers, Null-Zeichen zu senden (z. B. \0).
2	Durch dieses Flag wird SMTP anstelle von ESMTP verwendet.
6	Mit diesem Flag können Mailer eine Kopfzeile auf 7 Bit reduzieren.

Zusätzliche Gleichsetzungen für Delivery Agents ab Version 8.12 von sendmail

In der folgenden Tabelle werden zusätzliche Gleichsetzungen beschrieben, die Sie zusammen mit dem M-Definitionsbefehl für Delivery Agents verwenden können. Die folgende Syntax zeigt, wie neue Gleichsetzungen oder neue Argumente den Gleichsetzungen, die bereits in der Konfigurationsdatei vorhanden sind, hinzugefügt werden.

Magent-name, *equate*, *equate*, ...

Im folgenden Beispiel wird die neue W=-Gleichsetzung verwendet. Diese Gleichsetzung gibt die maximale Wartezeit bis zur Rückgabe des Mailers an, nachdem alle Daten gesendet wurden.

```
Msmtp, P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990, W=2m
```

Wenn Sie die Definition eines Werts für die m4-Konfiguration ändern möchten, verwenden Sie die Syntax aus dem folgenden Beispiel:

```
define('SMTP_MAILER_MAXMSGS', '1000')
```

Im vorangegangenen Beispiel ist die Anzahl der Nachrichten, die pro Verbindung mit einem smtp-Mailer übermittelt werden, auf 1000 begrenzt.

Informationen zum Erstellen einer neuen sendmail.cf-Datei finden Sie unter „Ändern der sendmail-Konfiguration“ auf Seite 313 in Kapitel 13, „Mailservices (Aufgaben)“.

Hinweis – Die Gleichsetzungsdefinitionen im mailer-Verzeichnis werden in der Regel nur geändert, um die Einstellungen zu optimieren.

TABELLE 14–28 Zusätzliche Gleichsetzungen für Delivery Agents

Gleichsetzung	Beschreibung
/=	Argument: Pfad eines Verzeichnisses Gibt ein Verzeichnis an, das für chroot() verwendet werden soll, bevor das Mailer-Programm ausgeführt wird.
m=	Argument: Einer der folgenden m4-Werte, die zuvor mit der define()-Routine definiert wurden. SMTP_MAILER_MAXMSGS für den smtp-Mailer LOCAL_MAILER_MAXMSGS für den local-Mailer RELAY_MAILER_MAXMSGS für den relay-Mailer Schränkt die Anzahl von Nachrichten ein, die pro Verbindung mit einem smtp-Mailer, einem local-Mailer oder einem relay-Mailer übermittelt werden.
W=	Argument: ein Zeitinkrement Gibt die maximale Wartezeit bis zur Rückgabe des Mailers an, nachdem alle Daten gesendet wurden.

Zusätzliche Warteschlangenfunktionen ab Version 8.12 von sendmail

In der folgenden Liste werden Informationen zu zusätzlichen Funktionen der Warteschlange aufgeführt.

- Diese Version unterstützt mehrere Warteschlangenverzeichnisse. Tragen Sie zur Verwendung mehrerer Warteschlangen in die Konfigurationsdatei einen QueueDirectory-Optionswert mit einem Sternchen (*) am Ende ein (siehe folgendes Beispiel).

  ```
  O QueueDirectory=/var/spool/mqueue/q*
  ```

  Der Optionswert, /var/spool/mqueue/q*, verwendet alle Verzeichnisse (oder symbolische Verknüpfungen mit Verzeichnissen), die mit "q" beginnen, als Warteschlangenverzeichnisse. Die Struktur des Warteschlangenverzeichnisses darf nicht geändert werden, während sendmail ausgeführt wird. Warteschlangenprozesse erzeugen einen separaten Prozess für die Ausführung der einzelnen Warteschlangen, es sei denn, das verbose-Flag (-v) wird für einen Nicht-Dämon-Warteschlangenprozess verwendet. Die neuen Elemente werden einer Warteschlange nach dem Zufallsprinzip zugewiesen.
- Das neue Datei-Naming-System für Warteschlangen verwendet Dateinamen, die 60 Jahre lang eindeutig sind. Mit diesem System können Warteschlangen-IDs ohne komplexe Dateisystemsperrungen zuzuweisen. Außerdem vereinfacht dieses System das Verschieben von Warteschlangenelementen zwischen den Warteschlangen.
- Ab Version 8.12 kann nur der root-Benutzer die Mailwarteschlange ausführen. Weitere Informationen finden Sie in den Beschreibungen der Änderungen auf der Manpage mailq(1). Neue aufgabenbezogene Informationen finden Sie unter „Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)“ auf Seite 336.
- Zur Umsetzung des Envelope-Splitting bestehen Dateinamen jetzt aus 15 Zeichen, nicht 14 Zeichen. Dateisysteme, deren Name auf 14 Zeichen beschränkt ist, werden nicht mehr unterstützt.

Aufgabenbezogene Informationen finden Sie unter „Verwalten der Warteschlangenverzeichnisse (Übersicht der Schritte)“ auf Seite 336.

Änderungen für LDAP ab Version 8.12 von sendmail

In der folgenden Liste werden die Änderungen bezüglich der Verwendung des LDAP (Lightweight Directory Access Protocol) in Verbindung mit sendmail beschrieben.

- Mit LDAPROUTE_EQUIVALENT() und LDAPROUTE_EQUIVALENT_FILE () können äquivalente Hostnamen angegeben werden, die durch den Maskierungs-Domainnamen für LDAP-Routing-Suchvorgänge ersetzt werden. Weitere Informationen finden Sie in der Datei /etc/mail/cf/README.

- Wie in den Versionshinweise erwähnt, die Teil der `sendmail` -Distribution auf `ftp://ftp.sendmail.org` sind, wurde die LDAPX-Map in LDAP umbenannt. Verwenden Sie für LDAP die folgende Syntax:

  `Kldap ldap` *options*
- Diese Version unterstützt die Rückgabe von mehreren Werten für einen einzelnen LDAP-Suchvorgang. Fügen Sie die Werte, die zurückgegeben werden sollen, wie folgt mithilfe der Option `-v` in eine durch Kommas getrennte Zeichenfolge ein.

  `Kldap ldap -v"`*mail*`,`*more-mail*`"`
- Wenn in der Deklaration einer LDAP-Map keine LDAP-Attribute angegeben sind, werden alle Attribute zurückgegeben, die in der Übereinstimmung gefunden werden.
- Diese Version von `sendmail` verhindert, dass ein einzelner Eintrag durch in Anführungszeichen eingeschlossene Kommas in Schlüssel- und Wertzeichenfolgen in den Spezifikationen der LDAP-Aliasdatei in mehrere Einträge aufgeteilt wird.
- Diese Version von `sendmail` bietet eine neue Option für LDAP-Maps. Mit der Option `-V`*separator* können Sie ein Trennzeichen angeben, sodass bei einem Suchvorgang sowohl ein Attribut als auch einen Wert zurückgegeben werden kann, die durch den entsprechenden *separator* getrennt werden.
- Neben dem `%s`-Token, das zum Analysieren einer LDAP-Filterspezifikation dient, können Sie das neue Token `%0` verwenden, um den Schlüsselpuffer zu verschlüsseln. Das Token `%0` verweist auf die eigentliche Bedeutung der LDAP-Sonderzeichen.

Das folgende Beispiel zeigt, wie sich die Funktionsweise dieser Token bei einem "*"-Suchvorgang unterscheidet.

TABELLE 14–29 Token-Vergleich

Spezifikation der LDAP-Map	Spezifikationsäquivalent	Ergebnis
`-k"uid=%s"`	`-k"uid=*"`	Stimmt mit jedem Datensatz überein, der ein Benutzerattribut aufweist.
`-k"uid=%0"`	`-k"uid=\2A"`	Stimmt mit einem Benutzer namens "*" überein.

In der folgenden Tabelle werden zusätzliche LDAP-Map-Flags beschrieben.

TABELLE 14–30 Zusätzliche LDAP-Map-Flags

Flag	Beschreibung
`-1`	Legt fest, dass nur eine einzige Übereinstimmung zurückgegeben wird. Wenn mehrere Übereinstimmungen zurückgegeben werden, entspricht das einem Suchergebnis, bei dem keine Datensätze gefunden wurden.

TABELLE 14–30 Zusätzliche LDAP-Map-Flags *(Fortsetzung)*

Flag	Beschreibung
`-r never|always|search|find`	Legt die LDAP-Alias-Dereferenzierungsoption fest.
`-Z size`	Begrenzt die Anzahl der Übereinstimmungen, die zurückgegeben werden.

Änderung am integrierten Mailer ab Version 8.12 von `sendmail`

Der alte integrierte `[TCP]`-Mailer steht nicht zur Verfügung. Verwenden Sie stattdessen den integrierten `P=[IPC]`-Mailer. Dank des integrierten Mailers für die Kommunikation zwischen Prozessen (`[IPC]`) können Nachrichten nun an einen UNIX-Domain-Socket auf Systemen übermittelt werden, die dies unterstützen. Sie können diesen Mailer in Verbindung mit `LMTP`-Delivery Agents verwenden, die einen festgelegten Socket überwachen. Ein Mailer kann wie folgt aussehen:

```
Mexecmail, P=[IPC], F=lsDFMmnqSXzA5@/:|, E=\r\n,
S=10, R=20/40, T=DNS/RFC822/X-Unix, A=FILE /var/run/lmtpd
```

Das erste Mailer-Argument im `[IPC]`-Mailer wird jetzt auf einen gültigen Wert geprüft. In der folgenden Tabelle sind mögliche Werte für das erste Mailer-Argument aufgeführt.

TABELLE 14–31 Mögliche Werte für das erste Mailer-Argument

Wert	Beschreibung
`A=FILE`	Für die UNIX-Domain-Socket-Übermittlung
`A=TCP`	Für TCP/IP-Verbindungen
`A=IPC`	Steht nicht mehr als erstes Mailer-Argument zur Verfügung

Zusätzliche Regellisten ab Version 8.12 von `sendmail`

In der folgenden Tabelle werden die zusätzlichen Regellisten sowie ihre Funktionsweise aufgeführt.

TABELLE 14–32 Neue Regellisten

Set	Beschreibung
`check_eoh`	Korreliert Informationen, die zwischen den Kopfzeilen erfasst werden, und prüft, ob Kopfzeilen fehlen. Diese Regelliste wird zusammen mit der Makrospeicher-Map verwendet und nach Erfassung aller Kopfzeilen aufgerufen.

TABELLE 14–32 Neue Regellisten *(Fortsetzung)*

Set	Beschreibung
check_etrn	Verwendet den ETRN-Befehl (wenn check_rcpt RCPT verwendet).
check_expn	Verwendet den EXPN-Befehl (wenn check_rcpt RCPT verwendet).
check_vrfy	Verwendet den VRFY-Befehl (wenn check_rcpt RCPT verwendet).

In der folgenden Liste werden zusätzliche Funktionen der Regellisten beschrieben.

- Nummerierte Regellisten haben auch Namen. Auf sie kann jedoch weiterhin über ihre Nummern zugegriffen werden.
- Mithilfe des H-Befehls der Kopfzeilenkonfiguration kann für die Prüfung von Kopfzeilen eine standardmäßige Regelliste festgelegt werden. Diese Regelliste wird nur aufgerufen, wenn einer Kopfzeile keine eigene Regelliste zugewiesen wurde.
- Kommentare in den Regellisten (d. h. Text, der in Klammern eingeschlossen ist) werden nicht entfernt, wenn es sich bei der Konfigurationsdateiversion um Version 9 oder höher handelt. Die folgende Regel stimmt beispielsweise mit der Eingabe `token (1)` und nicht mit der Eingabe `token` überein.

  ```
  R$+ (1)        $@ 1
  ```

- `sendmail` akzeptiert den SMTP-Befehl `RSET` auch dann, wenn es Befehle aufgrund der TCP-Wrapper oder der `check_relay`-Regelliste ablehnt.
- Eine Warnmeldung wird angezeigt, wenn Sie die `OperatorChars`-Option mehrmals aktivieren. Außerdem sollte `OperatorChars` nicht festgelegt werden, wenn die Regellisten bereits definiert sind.
- Der Name der Regelliste sowie ihre Zeilen werden ignoriert, wenn eine ungültige Regelliste deklariert wird. Die Zeilen der Regelliste werden `S0` nicht hinzugefügt.

Änderungen an Dateien ab Version 8.12 von `sendmail`

Beachten Sie die folgenden Änderungen:

- Ab Solaris 10 wurde zur Unterstützung eines schreibgeschützten `/usr`-Dateisystems der Inhalt des `/usr/lib/mail`-Verzeichnisses in das `/etc/mail/cf`-Verzeichnis verschoben. Weitere Informationen finden Sie unter „Inhalt des /etc/mail/cf-Verzeichnisses“ auf Seite 369. Beachten Sie jedoch, dass sich die Shell-Skripten `/usr/lib/mail/sh/check-hostname` und `/usr/lib/mail/sh/check-permissions` jetzt im Verzeichnis `/usr/sbin` befinden. Lesen Sie dazu „Weitere Dateien, die für Mailservices verwendet werden“ auf Seite 372. Zwecks Abwärtskompatibilität wurden symbolische Verknüpfungen erstellt, die auf die neuen Speicherorte der Dateien verweisen.
- Der neue Name von `/usr/lib/mail/cf/main-v7sun.mc` ist `/etc/mail/cf/cf/main.mc`.

- Der neue Name von /usr/lib/mail/cf/subsidiary-v7sun.mc ist /etc/mail/cf/cf/subsidiary.mc.
- Die helpfile befindet sich jetzt unter /etc/mail/helpfile. Der alte Name (/etc/mail/sendmail.hf) hat eine symbolische Verknüpfung, die auf den neuen Name verweist.
- Die trusted-users-Datei befindet sich jetzt unter /etc/mail/trusted-users. Wenn der alte Name (/etc/mail/sendmail.ct) während eines Upgrades erkannt wird, der neue Name aber nicht, wird eine harte Verknüpfung erstellt, die vom alten Namen auf den neuen Namen verweist. Anderenfalls wird keine Änderung vorgenommen. Der standardmäßige Inhalt ist root.
- Die local-host-names-Datei befindet sich jetzt unter /etc/mail/local-host-names. Wenn der alte Name (/etc/mail/sendmail.cw) während einer Aktualisierung erkannt wird, der neue Name aber nicht, wird eine harte Verknüpfung erstellt, die vom alten Namen auf den neuen Namen verweist. Anderenfalls wird keine Änderung vorgenommen. Die Länge des standardmäßigen Inhalts ist gleich null.

sendmail-Version 8.12 und IPv6-Adressen in der Konfiguration

Ab Version 8.12 von sendmail sollten in der Konfiguration verwendete IPv6-Adressen mithilfe des IPv6:-Tags mit einem Präfix versehen werden, um die Adresse richtig zu kennzeichnen. Wenn Sie eine IPv6-Adresse nicht identifizieren, wird kein Präfix-Tag verwendet.

TEIL V

Serielle Vernetzung – Themen

Dieser Abschnitt zur seriellen Vernetzung enthält eine Übersicht sowie aufgabenbezogene und Referenzinformationen über PPP und UUCP.

◆ ◆ ◆ KAPITEL 15

Solaris PPP 4.0 (Überblick)

In diesem Abschnitt werden Themen im Zusammenhang mit der seriellen Vernetzung behandelt. Bei der seriellen Vernetzung geht es um die Verwendung einer seriellen Schnittstelle, wie beispielsweise ein RS-232- oder V.35-Port. Über eine solche Schnittstelle wird eine Verbindung mit einem oder mehreren Computern zur Datenübertragung hergestellt. Anders als bei LAN-Schnittstellen (wie beispielsweise Ethernet) werden diese seriellen Schnittstellen verwendet, um Rechner zu verbinden, die durch große Entfernungen voneinander getrennt sind. PPP (Point-to-Point Protocol) und UUCP (UNIX-to-UNIX CoPy) sind spezielle Technologien, die zur Implementierung der seriellen Vernetzung eingesetzt werden können. Eine serielle Schnittstelle, die für die Vernetzung konfiguriert ist, wird für mehrere Benutzer verfügbar gemacht. Dies geschieht in ähnlicher Weise wie bei jeder anderen Netzwerkschnittstelle (beispielsweise Ethernet).

In diesem Kapitel wird Solaris PPP 4.0 vorgestellt. Mit dieser Version von PPP können zwei Computer an verschiedenen physischen Standorten mithilfe von PPP über zahlreiche Medien miteinander kommunizieren. Ab Solaris 9 ist Solaris PPP 4.0 ein Teil der Basisinstallation.

Folgende Themen werden behandelt:

- „Solaris PPP 4.0 – Grundlagen“ auf Seite 421
- „PPP-Konfigurationen und Terminologie“ auf Seite 425
- „PPP-Authentifizierung“ auf Seite 431
- „Unterstützung für DSL-Benutzer durch PPPoE“ auf Seite 433

Solaris PPP 4.0 – Grundlagen

Solaris PPP 4.0 implementiert PPP (Point-to-Point Protocol), ein Datenverbindungsprotokoll, das zur Familie der TCP/IP-Protokolle gehört. PPP beschreibt, wie Daten zwischen zwei Endpunktrechnern über Kommunikationsmedien wie beispielsweise Telefonleitungen übertragen werden.

Seit den frühen 1990er Jahren ist PPP ein weitverbreiteter Internetstandard zum Senden von Datagrammen über eine Kommunikationsverbindung. Der PPP-Standard wird in RFC 1661 von der Point-to-Point Working Group der IETF (Internet Engineering Task Force) beschrieben. PPP wird eingesetzt, wenn Remote-Computer einen ISP (Internet Service Provider) oder einen Unternehmensserver aufrufen, der für eingehende Aufrufe konfiguriert ist.

Solaris PPP 4.0 basiert auf dem öffentlichen ANU (Australian National University) PPP-2.4 und implementiert den PPP-Standard. Sowohl asynchrone als auch synchrone PPP-Verbindungen werden unterstützt.

Solaris PPP 4.0-Kompatibilität

Die verschiedenen Versionen des Standard-PPP sind in der Internet-Community weitverbreitet. ANU PPP-2.4 wird häufig für Linux, Tru64 UNIX und die drei wichtigsten BSD-Varianten eingesetzt:

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0 bietet bestens konfigurierbare Funktionen von ANU PPP-2.4 für Rechner, auf denen das Betriebssystem Solaris ausgeführt wird. Rechner, auf denen Solaris PPP 4.0 ausgeführt wird, ermöglichen die problemlose Herstellung von PPP-Verbindungen mit jedem Rechner, auf dem eine Implementierung des Standard-PPP ausgeführt wird.

Zu den nicht auf ANU basierten PPP-Implementierungen, die mit Solaris PPP 4.0 harmonieren, zählen:

- Solaris PPP, auch bekannt als `asppp`, ist zusammen mit Solaris 2.4 bis 8 erhältlich.
- Solstice PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0 (synchron)

Zu verwendende Version von Solaris PPP

Solaris PPP 4.0 wird unterstützt. In Solaris 9 und höher ist die frühere Version der asynchronen Solaris PPP-Software `asppp` nicht enthalten. Weitere Informationen finden Sie hier:

- Kapitel 23, „Migrieren von Asynchronous Solaris PPP zu Solaris PPP 4.0 (Aufgaben)“
- Die Solaris System Administrator Collection finden Sie unter http://docs.sun.com

Vorteile von Solaris PPP 4.0

Wenn Sie zurzeit `asppp` verwenden, sollten Sie eine Migration zu Solaris PPP 4.0 in Erwägung ziehen. Beachten Sie die Unterschiede zwischen den beiden Solaris PPP-Technologien:

- **Übertragungsmodi**

  `asppp` unterstützt nur die asynchrone Kommunikation. Solaris PPP 4.0 unterstützt sowohl die asynchrone als auch die synchrone Kommunikation.

- **Konfigurationsprozess**

  Um `asppp` einzurichten, müssen die `asppp.cf` -Konfigurationsdatei, drei UUCP-Dateien und der Befehl `ifconfig` konfiguriert werden. Außerdem müssen die Schnittstellen für alle Benutzer vorkonfiguriert werden, die sich eventuell bei einem Rechner anmelden.

  Zum Einrichten von Solaris PPP 4.0 ist es erforderlich, Optionen für die PPP-Konfigurationsdateien zu definieren oder den `pppd`-Befehl mit Optionen anzugeben. Sie können auch eine Kombination aus der Konfigurationsdatei und dem Befehlszeilenverfahren verwenden. Mit Solaris PPP können Schnittstellen dynamisch erstellt und entfernt werden. Es ist nicht nötig, PPP-Schnittstellen direkt für jeden Benutzer zu konfigurieren.

- **Solaris PPP 4.0-Funktionen, die nicht in asppp verfügbar sind**
  - MS-CHAPv1- und MS-CHAPv2-Authentifizierung
  - PPP over Et0hernet (PPPoE) zur Unterstützung von ADSL-Brücken
  - PAM-Authentifizierung
  - Plug-in-Module
  - IPv6-Adressierung
  - Datenkomprimierung mit Deflate oder BSD-Komprimierung
  - Clientseitige Callback-Unterstützung von Microsoft

Solaris PPP 4.0-Upgradepfad

Wenn Sie eine vorhandene `asppp`-Konfiguration auf Solaris PPP 4.0 umstellen, können Sie das Übersetzungsskript verwenden, das in dieser Version enthalten ist. Eine umfassende Anleitung finden Sie unter „So konvertieren Sie von `asppp` in Solaris PPP 4.0“ auf Seite 575.

Weitere Informationen zu PPP

Viele Ressourcen mit Informationen über PPP sind in Publikationen und online zu finden. Die folgenden Unterabschnitte enthalten Hinweise und Orientierungshilfen.

Professionelle Referenzpublikationen über PPP

Weitere Informationen zu gebräuchlichen PPP-Implementierungen, darunter ANU PPP, finden Sie in den folgenden Büchern:

- Carlson, James. *PPP Design, Implementation, and Debugging*. 2nd ed. Addison-Wesley, 2000.
- Sun, Andrew. *Using and Managing PPP*. O'Reilly & Associates, 1999.

Websites über PPP

Auf den folgenden Websites finden Sie allgemeine Informationen über PPP:

- Technische Informationen, häufig gestellte Fragen (FAQs), Diskusssionen über die Solaris-Systemverwaltung und frühere Versionen von PPP finden Sie auf der Website für Systemadministratoren unter http://www.sun.com/bigadmin/home/index.html .
- Informationen zur Modemkonfiguration und Empfehlungen für viele verschiedene Implementierungen finden Sie auf der Website für Webprojektmanagement und Softwareentwicklung von Stokely Consulting unter http://www.stokely.com/unix.serial.port.resources/ppp.slip.html.

RFCs (Requests for Comments) über PPP

Einige der hilfreichen Internet-RFCs über PPP sind:

- 1661 und 1662, in denen die wichtigsten Funktionen von PPP beschrieben sind.
- 1334, in dem Authentifizierungsprotokolle wie beispielsweise das PAP (Password Authentication Protocol) und CHAP (Challenge-Handshake Authentication Protocol) beschrieben sind.
- 1332, ein informatives RFC, in dem PPPoE (PPP over Ethernet) beschrieben wird.

Um Kopien von PPP-RFCs anzufordern, geben Sie die entsprechenden RFC-Nummern auf der IETF-RFC-Webseite unter http://www.ietf.org/rfc.html an.

Manpages über PPP

Technische Informationen zur Solaris PPP 4.0-Implementierung finden Sie auf den folgenden Manpages:

- `pppd`(1M)
- `chat`(1M)
- `pppstats`(1M)
- `pppoec`(1M)
- `pppoed`(1M)
- `sppptun`(1M)
- `snoop`(1M)

Sie können sich auch auf der Manpage für `pppdump`(1M) informieren. PPP-bezogene Manpages können Sie mit dem Befehl `man` aufrufen.

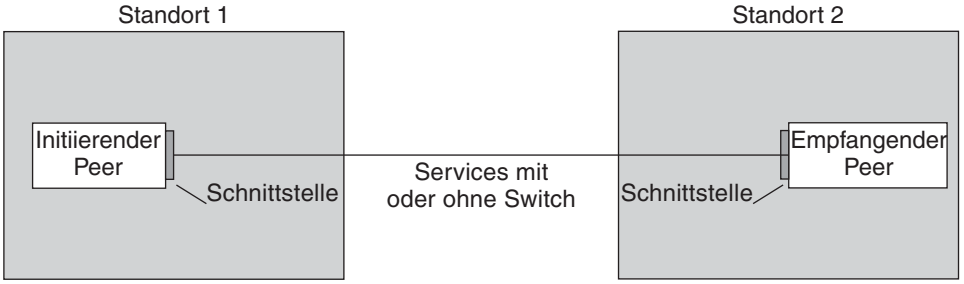
PPP-Konfigurationen und Terminologie

In diesem Abschnitt werden PPP-Konfigurationen vorgestellt. Außerdem werden Begriffe definiert, die in dieser Anleitung verwendet werden.

Solaris PPP 4.0 unterstützt eine Reihe von Konfigurationen.

- Wählzugangs- oder *Einwahlverbindung*skonfigurationen
- Festverdrahtungs- oder *Standleitung*skonfigurationen

ABBILDUNG 15–1 Teile der PPP-Verbindung



Die obenstehende Abbildung zeigt eine einfache PPP-Verbindung. Die Verbindung besteht aus folgenden Teilen:

- Zwei Rechner, die sich normalerweise an verschiedenen physischen Standorten befinden und als *Peers* bezeichnet werden. Ein Peer kann je nach standortspezifischen Anforderungen ein PC, eine Workstation, ein großer Server oder auch ein geschäftlicher Router sein.
- Serielle Schnittstelle auf jedem Peer. Auf Solaris-Rechnern kann diese Schnittstelle `cua`, `hihp` oder eine andere Schnittstelle sein. Dies hängt davon ab, ob ein asynchrones oder synchrones PPP konfiguriert wird.
- Eine physische Verbindung wie beispielsweise ein serielles Kabel, eine Modemverbindung oder eine Standleitung eines Netzbetreibers (T1- oder T3-Leitung).

PPP-Einwahlverbindung – Übersicht

Die gebräuchlichste PPP-Konfiguration ist die *Wählverbindung*. Bei einer Einwahlverbindung *wählt* der lokale Peer den Remote-Peer an, um eine Verbindung herzustellen und PPP

auszuführen. Während des Wählvorgangs wählt der lokale Peer die Telefonnummer des Remote-Peers, um eine Verbindung herzustellen.

In einem normalen Wählszenario wählt ein Heimcomputer einen Peer eines ISP an, der eingehende Anrufe empfängt. Ein anderes Szenario ist ein Unternehmensstandort mit einem lokalen Rechner, der Daten über eine PPP-Verbindung an einen Peer in einem anderen Gebäude sendet.

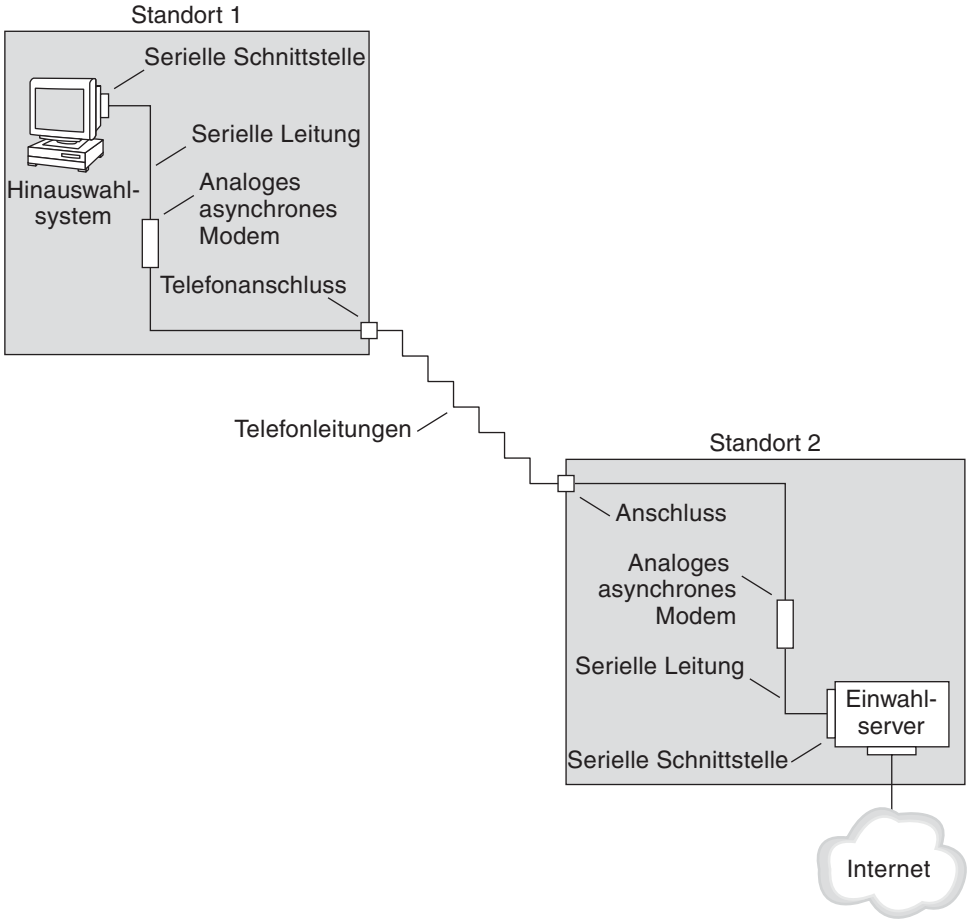
In dieser Anleitung wird der lokale Peer, der die Wählverbindung initiiert, als *Hinauswahlrechner* bezeichnet. Der Peer, der den eingehenden Aufruf empfängt, wird als *Einwahlserver* bezeichnet. Dieser Rechner ist der Ziel-Peer des Hinauswahlrechners und kann ein echter Server sein.

PPP ist kein Client-Server-Protokoll. In manchen PPP-Dokumenten werden die Begriffe "Client" und "Server" verwendet, um den Aufbau einer Wählverbindung zu beschreiben. Ein Einwahlserver ist kein echter Server wie beispielsweise ein Dateiserver oder Namenserver. Ein Einwahlserver ist ein häufig gebrauchter PPP-Begriff, da Einwahlsysteme oft den Netzwerkzugang für mehrere Hinauswahlrechner bereitstellen. Dennoch ist der Einwahlserver der Ziel-Peer des Hinauswahlrechners.

Teile der PPP-Einwahlverbindung

Siehe folgende Abbildung:

ABBILDUNG 15–2 Einfache analoge PPP-Wählverbindung



Die Konfiguration für Standort 1 (die Hinauswahlseite der Verbindung) besteht aus folgenden Elementen:

- Hinauswahlrechner, normalerweise ein PC oder eine Workstation in einem Privathaushalt
- Serielle Schnittstelle auf dem Hinauswahlrechner `/dev/cua/a` oder `/dev/cua/b` ist die standardmäßige serielle Schnittstelle für abgehende Anrufe auf Rechnern, auf denen Solaris-Software ausgeführt wird.
- Asynchrones Modem oder ISDN-Terminal-Adapter (TA), der an eine Telefonbuchse angeschlossen ist
- Telefonleitungen und Services einer Telefongesellschaft

Die Konfiguration für Standort 2 (die Einwahlseite der Verbindung) besteht aus folgenden Elementen:

- Telefonbuchse oder ähnlicher Anschluss, der mit dem Telefonnetz verbunden ist
- Asynchrones Modem oder ISDN-TA
- Serielle Schnittstelle auf dem Einwahlserver, entweder `ttya` oder `ttyb` für eingehende Anrufe
- Einwahlserver, der mit einem Netzwerk verbunden ist, beispielsweise ein Unternehmens-Intranet oder das globale Internet im Falle eines ISP

Verwenden eines ISDN-Terminal-Adapters mit einem Hinauswahlrechner

Externe ISDN-Terminal-Adapter sind schneller als Modems, werden aber im Grunde in gleicher Weise konfiguriert. Der Hauptunterschied beim Konfigurieren eines ISDN-TA ist das Chat-Skript, für das herstellerspezifische TA-Befehle erforderlich sind. Weitere Informationen zu Chat-Skripten für ISDN-TAs finden Sie unter „Chat-Skript für einen externen ISDN-TA“ auf Seite 545.

Vorgänge während der Einwahlkommunikation

Die PPP-Konfigurationsdateien auf den Hinauswahl- und Einwahl-Peers enthalten Anweisungen für das Einrichten der Verbindung. Die folgenden Vorgänge finden statt, wenn eine Einwahlverbindung initiiert wird:

1. Der Benutzer oder der Prozess auf dem Hinauswahlrechner führt den Befehl `pppd` aus, um die Verbindung aufzubauen.
2. Der Hinauswahlrechner liest die PPP-Konfigurationsdateien. Der Hinauswahlrechner sendet Anweisungen (einschließlich der Telefonnummer des Einwahlservers) über die serielle Verbindung an das Modem.
3. Das Modem wählt die Telefonnummer, um eine Telefonverbindung mit dem Modem des Einwahlservers herzustellen.

   Die Textzeichenfolgen, die der Hinauswahlrechner an das Modem und den Einwahlserver sendet, sind in einer Datei enthalten, die als *Chat-Skript* bezeichnet wird. Der Hinauswahlrechner sendet bei Bedarf Befehle an den Einwahlserver, um PPP auf dem Server aufzurufen.
4. Das am Einwahlserver angeschlossene Modem beginnt, eine Verbindung mit dem Modem des Hinauswahlrechners auszuhandeln.
5. Wenn die Aushandlung zwischen den Modems abgeschlossen ist, gibt der Hinauswahlrechner die Meldung "CONNECT" aus.
6. Das PPP auf beiden Peers tritt in die Phase des Verbindungsaufbaus ein, in der das LCP (Link Control Protocol) die grundlegenden Verbindungsparameter und die Verwendung der Authentifizierung aushandelt.

7. Die Peers authentifizieren sich bei Bedarf gegenseitig.
8. Die NCPs (Network Control Protocols) des PPP handeln die Verwendung der Netzwerkprotokolle wie beispielsweise IPv4 oder IPv6 aus.

Der Hinauswahlrechner kann dann `telnet` oder einen ähnlichen Befehl an einen Host übermitteln, der über den Einwahlserver erreichbar ist.

PPP-Standleitung – Übersicht

Eine festverdrahtete PPP-*Standleitungs*-Konfiguration besteht aus zwei miteinander verbundenen Peers. Diese Verbindung besteht aus einem geschalteten oder nicht geschalteten digitaler Service eines Providers. Solaris PPP 4.0 kommuniziert über jedes Point-to-Point-Standleitungsmedium mit Vollduplex. Normalerweise mietet ein Unternehmen eine festverdrahtete Verbindung von einem Netzbetreiber, um eine Verbindung mit einem ISP oder einem anderen Remote-Standort herzustellen.

Vergleich von Wählverbindungen und Standleitungsverbindungen

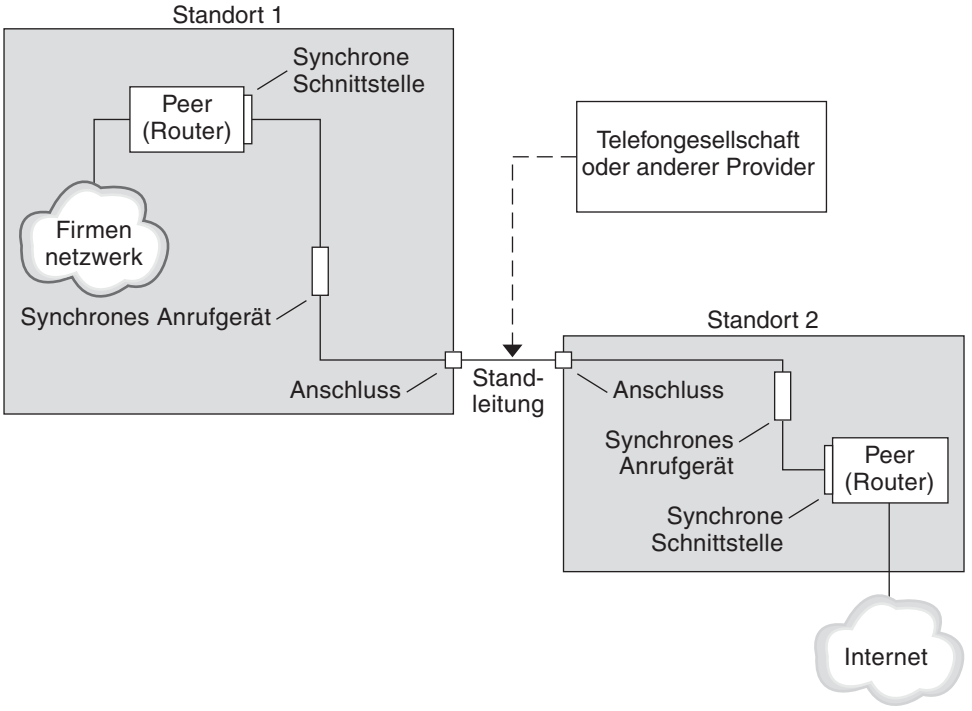
Für sowohl Wählverbindungen als auch Standleitungsverbindungen werden zwei Peers benötigt, die durch ein Kommunikationsmedium verbunden sind. In der nachstehenden Tabelle sind die Unterschiede zwischen den Verbindungsarten zusammengefasst.

Standleitungsverbindung	Wählverbindung
Es besteht stets eine Verbindung, es sei denn, die Standleitung wird durch einen Systemadministrator oder einen Stromausfall außer Betrieb gesetzt.	Wird nach Bedarf aufgebaut, wenn ein Benutzer versucht, einen Remote-Peer aufzurufen.
Synchrone und asynchrone Kommunikation. Für die asynchrone Kommunikation wird oft ein Fernübertragungsmodem eingesetzt.	Asynchrone Kommunikation
Von einem Provider gemietet.	Es werden vorhandene Telefonleitungen verwendet.
Es werden synchrone Geräte benötigt.	Es werden weniger teure Modems verwendet.
Es werden synchrone Ports benötigt, die bei den meisten SPARC-Systemen eingesetzt werden. Synchrone Ports werden jedoch weder für x86-Systeme noch neuere SPARC-Systeme eingesetzt.	Es werden standardmäßige serielle Schnittstellen verwendet, die bei den meisten Computern vorhanden sind.

Teile einer PPP-Standleitungsverbindung

Siehe folgende Abbildung:

ABBILDUNG 15–3 Standleitungskonfiguration



Die Standleitungsverbindung besteht aus folgenden Teilen:

- **Zwei Peers**, jeder an einem Ende der Leitung. Jeder Peer kann eine Workstation oder ein Server sein. Oft fungiert ein Peer als Router zwischen seinem Netzwerk oder dem Internet und dem Peer am anderen Ende der Leitung.
- **Synchrone Schnittstelle auf jedem Peer**. Für manche Rechner, auf denen die Solaris-Software ausgeführt wird, müssen Sie eine synchrone Schnittstellenkarte wie HSI/P kaufen, um eine Verbindung mit einer Standleitung herstellen zu können. Andere Rechner, wie etwa UltraSPARC -Workstations, haben integrierte synchrone Schnittstellen.
- **CSU/DSU-synchrones digitales Gerät auf jedem Peer**, das den synchronen Port mit der Standleitung verbindet.

  Ein CSU kann je nach Gebietsschema in das DSU integriert sein, in Ihrem Besitz sein oder von einem Provider gemietet werden. Das DSU stellt für den Solaris-Rechner eine standardmäßige synchrone serielle Schnittstelle bereit. Mit Frame Relay führt das FRAD (Frame Relay Access Device) die Anpassung der seriellen Schnittstelle durch.
- **Standleitung** für geschaltete und nicht geschaltete digitale Services, z. B. SONET/SDH, Frame Relay PVC und T1.

Vorgänge während der Standleitungskommunikation

Bei den meisten Standleitungen findet keine Anwahl zwischen den Peers statt. Stattdessen nutzen Unternehmen Standleitungsservices, um zwei feste Standorte zu verbinden. Die beiden Peers an den Enden der Standleitung können sich an verschiedenen physischen Standorten desselben Unternehmens befinden. Auch kann ein Unternehmen einen Router für eine Standleitung installieren, die mit einem ISP verbunden ist.

Standleitungen sind weniger gebräuchlich als Wählverbindungen, obwohl festverdrahtete Verbindungen einfacher eingerichtet werden können. Für festverdrahtete Verbindungen sind keine Chat-Skripten erforderlich. Die Authentifizierung wird oft nicht verwendet, weil beide Peers, die über eine Standleitung kommunizieren, einander bekannt sind. Nachdem die beiden Peers PPP über die Verbindung initiiert haben, bleibt die Verbindung aktiv. Eine Standleitungsverbindung bleibt aktiv, bis sie ausfällt oder von einem der beiden Peers beendet wird.

Ein Peer an einer Standleitung, auf dem Solaris PPP 4.0 ausgeführt wird, verwendet größtenteils dieselben Konfigurationsdateien, die eine Einwahlverbindung definieren.

Durch den folgenden Vorgang wird die Kommunikation über die Standleitung initiiert:

1. Jeder Peer führt den Befehl `pppd` als Teil des Boot-Vorgangs oder eines anderen Systemverwaltungsskripts aus.
2. Die Peers lesen ihre PPP-Konfigurationsdateien.
3. Die Peers handeln Kommunikationsparameter aus.
4. Eine IP-Verbindung wird hergestellt.

PPP-Authentifizierung

Die *Authentifizierung* ist ein Verifizierungsvorgang, der von einem Benutzer durchgeführt wird, um seine Identität zu bestätigen. Die UNIX-Anmeldesequenz ist eine einfache Form der Authentifizierung:

1. Über den Befehl `login` wird der Benutzer zur Eingabe eines Namens und eines Passworts aufgefordert.
2. Anschließend wird über `login` versucht, den Benutzer zu authentifizieren, indem in der Passwortdatenbank nach dem eingegebenen Benutzernamen und dem Passwort gesucht wird.
3. Sind Benutzername und Passwort in der Datenbank enthalten, wird der Benutzer *authentifiziert* und erhält Zugang zum System. Sind Benutzername und Passwort nicht in der Datenbank enthalten, wird dem Benutzer der Zugang zum System verwehrt.

Standardmäßig verlangt Solaris PPP 4.0 keine Authentifizierung für Rechner, bei denen keine standardmäßige Route angegeben ist. Aus diesem Grund werden aufrufende

Remote-Programme nicht von lokalen Rechnern authentifiziert, die keine standardmäßige Route haben. Umgekehrt verhält es sich bei Rechnern mit standardmäßig definierter Route: aufrufende Remote-Programme werden stets authentifiziert.

Sie können PPP-Authentifizierungsprotokolle verwenden, um die Identität von aufrufenden Programmen zu verifizieren, die versuchen, eine PPP-Verbindung mit Ihrem Rechner herzustellen. Wenn Ihr lokaler Rechner zum Authentifizieren von aufrufenden Programmen jedoch Peers aufrufen muss, müssen Sie die PPP-Authentifizierungsinformationen konfigurieren.

Authentifizierer und Authentifizierungsempfänger

Der aufrufende Rechner in einer PPP-Verbindung wird als *Authentifizierungsempfänger* betrachtet, da der aufrufende Rechner seine Identität gegenüber dem Remote-Peer nachweisen muss. Der Peer wird als *Authentifizierer* betrachtet. Der Authentifizierer sucht in den entsprechenden PPP-Dateien nach dem Sicherheitsprotokoll, um die Identität des aufrufenden Rechners zu prüfen und den aufrufenden Rechner zu authentifizieren.

Für eine Wählverbindung konfigurieren Sie normalerweise die PPP-Authentifizierung. Wenn der Aufruf gestartet wird, ist der Hinauswahlrechner der Authentifizierungsempfänger. Der Einwahlserver ist der Authentifizierer. Der Server verfügt über eine Datenbank in Form einer Geheimnisdatei (*secrets*-Datei). In dieser Datei sind alle Benutzer aufgelistet, die berechtigt sind, eine PPP-Verbindung mit dem Server herzustellen. Diese Benutzer sind *vertrauenswürdige aufrufende Programme*.

Manche Hinauswahlrechner verlangen von Remote-Peers die Bereitstellung von Authentifizierungsinformationen, wenn diese auf einen Aufruf eines Hinauswahlrechners antworten. Dann findet ein Rollentausch statt: Der Remote-Peer wird zum Authentifizierungsempfänger und der Hinauswahlrechner zum Authentifizierer.

Hinweis – PPP 4.0 verhindert nicht die Authentifizierung durch Standleitungs-Peers. Die Authentifizierung wird jedoch nicht häufig für Standleitungsverbindungen eingesetzt. Es liegt in der Natur von Standleitungen, dass die Teilnehmer an beiden Enden einer Standleitung einander bekannt sind. Beide Teilnehmer sind oft vertrauenswürdig. Da die PPP-Authentifizierung jedoch einfach realisierbar ist, sollten Sie eine Authentifizierung für Standleitungen ernsthaft in Erwägung ziehen.

PPP-Authentifizierungsprotokolle

Die PPP-Authentifizierungsprotokolle sind PAP (Password Authentication Protocol) und CHAP (Challenge-Handshake Authentication Protocol). Jedes Protokoll verwendet eine *Geheimnis*-Datenbank, die Identifizierungsinformationen oder

Sicherheitsberechtigungsnachweise für jedes aufrufende Programm enthält, das berechtigt ist, eine Verbindung mit dem lokalen Rechner herzustellen. Eine ausführliche Erläuterung zu PAP finden Sie unter „PAP (Password Authentication Protocol)“ auf Seite 549. Eine Erläuterung zu CHAP finden Sie unter „CHAP (Challenge-Handshake Authentication Protocol)“ auf Seite 552.

Warum die PPP-Authentifizierung verwendet werden sollte

Die Authentifizierung für eine PPP-Verbindung ist optional. Obwohl anhand der Authentifizierung verifiziert werden kann, dass ein Peer vertrauenswürdig ist, wird für die Vertraulichkeit der Daten nicht garantiert. Zu diesem Zweck verwenden Sie Verschlüsselungssoftware wie IPsec, PGP, SSL, Kerberos oder Solaris Secure Shell.

Hinweis – Solaris PPP 4.0 implementiert nicht das in RFC 1968 beschriebene PPP ECP (Encryption Control Protocol).

In folgenden Fällen sollte die PPP-Authentifizierung in Betracht gezogen werden:

- Ihr Unternehmen akzeptiert eingehende Anrufe von Benutzern, die über das öffentliche geschaltete Telefonnetz eingehen.
- Die Sicherheitsrichtlinien Ihres Unternehmens verlangen von Remote-Benutzern Authentifizierungs-Berechtigungsnachweise, wenn diese Benutzer über eine Unternehmens-Firewall auf Ihr Netzwerk zugreifen oder gesicherte Transaktion einleiten.
- Sie können aufrufende Programme mithilfe einer standardmäßigen UNIX-Passwortdatenbank wie `/etc/passwd`, NIS, NIS+, LDAP, oder PAM authentifizieren. Verwenden Sie hierfür die PAP-Authentifizierung.
- Die Einwahlserver Ihres Unternehmens stellen auch die Internetverbindung des Netzwerks bereit. Verwenden Sie hierfür die PAP-Authentifizierung.
- Die serielle Verbindung ist weniger sicher als die Passwortdatenbank des Rechners oder in den Netzwerken an den beiden Enden der Verbindung. Verwenden Sie hierfür die CHAP-Authentifizierung.

Unterstützung für DSL-Benutzer durch PPPoE

Viele Netzbetreiber und Personen, die von zu Hause aus arbeiten, nutzen die DSL-Technologie (Digital Subscriber Line), um schnell auf das Netzwerk zugreifen zu können. Solaris PPP 4.0 umfasst PPPoE (PPP over Ethernet) zur Unterstützung von DSL-Benutzern. Mit PPPoE können PPP-Sitzungen ausgeführt werden, in denen mehrere Hosts über eine Ethernet-Verbindung mit einem oder mehreren Zielsystemen kommunizieren.

Wenn einer der folgenden Faktoren für Ihr Unternehmen zutrifft, sollten Sie PPPoE verwenden:

- Sie unterstützen DSL-Benutzer (möglicherweise gehören Sie selbst dazu). Ihr DSL-Serviceprovider verlangt von den Benutzern, einen PPPoE-Tunnel zu konfigurieren, um die über die DSL-Verbindung angebotenen Services nutzen zu können.
- Ihr Unternehmen nutzt die Services eines ISP, der beabsichtigt, seinen Kunden PPPoE anzubieten.

Dieser Abschnitt enthält Erläuterungen von PPPoE-Begriffen sowie eine Übersicht einer grundlegenden PPPoE-Topologie.

PPPoE – Übersicht

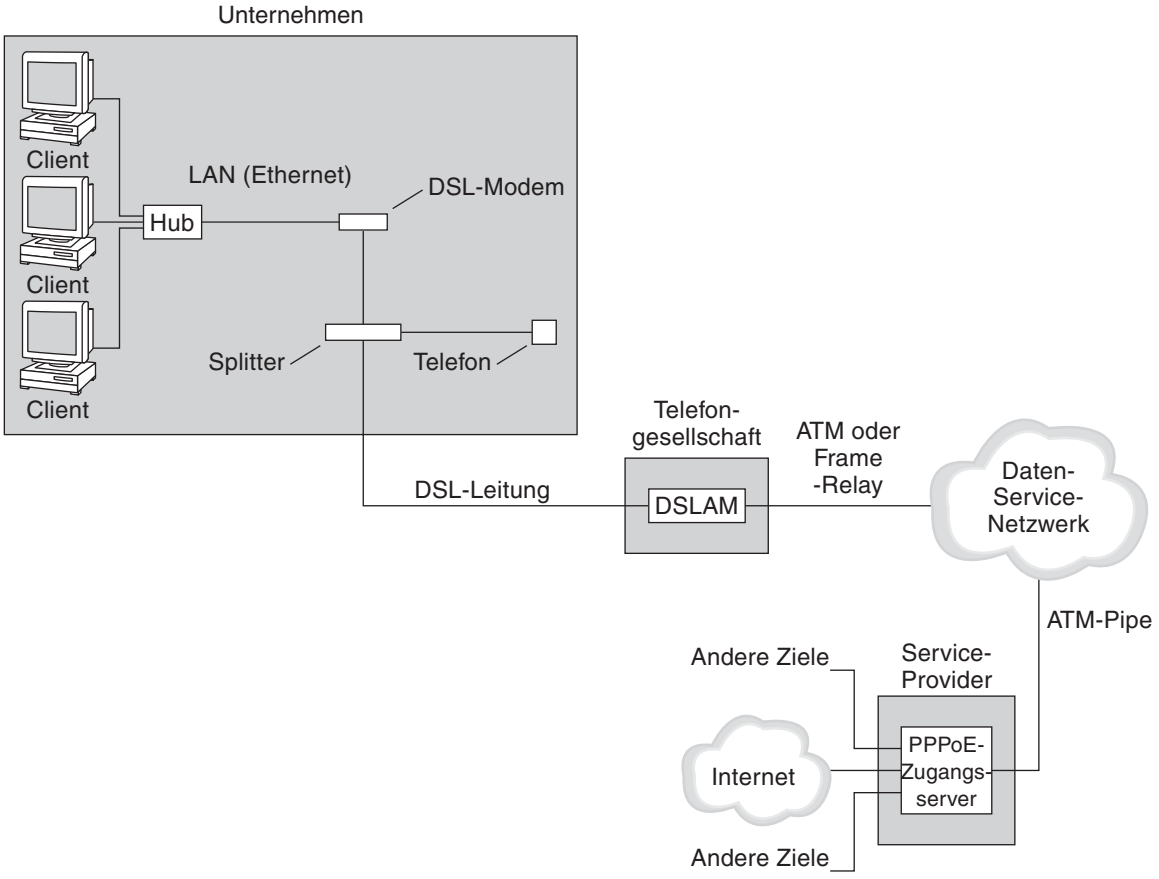
PPPoE ist ein gesetzlich geschütztes Protokoll von RedBack Networks. PPPoE ist ein Erkennungsprotokoll, wodurch es sich von anderen standardmäßigen PPP-Versionen unterscheidet. In einem PPPoE-Szenario muss ein Rechner, der die PPP-Kommunikation initiiert, zunächst einen Peer lokalisieren bzw. *erkennen*, der PPPoE ausführt. Das PPPoE-Protokoll verwendet Ethernet-Broadcast-Pakete, um den Peer zu lokalisieren.

Nach dem Erkennungsprozess richtet PPPoE einen Ethernet-basierten Tunnel ein, der vom initiierenden Host (oder *PPPoE-Client*) zum Peer (*PPPoE-Zugangsserver*) führt. *Tunneling* ist ein Verfahren, bei dem ein Protokoll auf einem anderen Protokoll ausgeführt wird. Solaris PPP 4.0 erstellt einen Tunnel zu PPP over Ethernet IEEE 802.2 mithilfe von PPPoE her. Beide Protokolle sind Datenverbindungsprotokolle. Die daraus resultierende PPP-Verbindung verhält sich wie eine dedizierte Verbindung zwischen dem PPPoE-Client und dem Zugangsserver. Ausführliche Informationen zu PPPoE finden Sie unter „Erstellen von PPPoE-Tunneln für DSL-Unterstützung“ auf Seite 558.

Teile einer PPPoE-Konfiguration

Zu einer PPP-Konfiguration gehören drei Teilnehmer: ein Konsument, eine Telefongesellschaft und ein Serviceprovider (siehe nachstehende Abbildung).

ABBILDUNG 15–4 Teilnehmer eines PPPoE-Tunnels



PPPoE-Kunden

Als Systemadministrator unterstützen Sie möglicherweise Konsumenten beim Einrichten von PPPoE-Konfigurationen. Ein typischer PPPoE-Konsument ist eine Person, die PPPoE über eine DSL-Verbindung nutzt. Ein weiterer PPPoE-Konsument kann ein Unternehmen sein, deren Mitarbeiter über eine gekaufte DSL-Leitung PPPoE-Tunnel ausführen (siehe obenstehende Abbildung).

Der Hauptgrund, warum Firmenkonsumenten PPPoE verwenden, ist die PPP-Kommunikation mit verschiedenen Hosts über ein Hochgeschwindigkeits-DSL-Gerät. Oft verwendet ein einzelner PPPoE-Client ein bestimmtes *DSL-Modem*. Außerdem kann ein DSL-Modem, das durch eine Ethernet-Verbindung mit einem Hub verbunden ist, von einer Gruppe von Clients auf einem Hub verwendet werden.

Hinweis – Aus technischer Sicht sind DSL-Geräte keine Modems, sondern Brücken. Da diese Geräte jedoch allgemein als Modems bezeichnet werden, wird in dieser Anleitung der Begriff "DSL-Modem" verwendet.

PPPoE führt PPP über einen Tunnel in der Ethernet-Leitung aus, die mit dem DSL-Modem verbunden ist. Diese Leitung ist mit einem Splitter verbunden, der wiederum mit einer Telefonleitung verbunden ist.

PPPoE in einer Telefongesellschaft

Die Telefongesellschaft ist das Mittelstück im PPPoE-Szenario. Die Telefongesellschaft teilt das über die Telefonleitung empfangene Signal. Hierzu wird ein Gerät verwendet, das als *DSLAM (Digital Subscriber Line Access Multiplexer)* bezeichnet wird. Das DSLAM verteilt die Signale auf separate Leitungen, d. h. analoge Leitungen für Telefonservices und digitale Leitungen für PPPoE. Vom DSLAM aus führen die digitalen Leitungen den Tunnel über ein ATM-Datennetzwerk zum ISP.

PPPoE bei einem Serviceprovider

Der ISP empfängt die PPPoE-Übertragung vom ATM-Datennetzwerk über eine Brücke. Beim ISP fungiert ein Zugangsserver als Peer für die PPP-Verbindung, um PPPoE-Funktionen auszuführen. Der Zugangsserver ähnelt in seiner Funktionsweise sehr dem Einwahlserver (siehe Abbildung 15–2). Allerdings verwendet der Zugangsserver keine Modems. Der Zugangsserver wandelt die PPPoE-Sitzungen in normalen IP-Verkehr um, beispielsweise für den Internetzugang.

Wenn Sie ein Systemadministrator eines ISP sind, sind Sie möglicherweise für die Konfiguration und Verwaltung eines Zugangsservers verantwortlich.

Sicherheit eines PPPoE-Tunnels

Der PPPoE-Tunnel ist grundsätzlich unsicher. Sie können PAP oder CHAP verwenden, um eine Benutzerauthentifizierung für die PPP-Verbindung bereitzustellen, die über den Tunnel läuft.

◆ ◆ ◆ KAPITEL 16

PLanen einer PPP-Verbindung (Aufgaben)

Mit dem Einrichten einer PPP-Verbindung sind verschiedene separate Aufgaben verbunden, darunter Planungsaufgaben und Aktivitäten, die nicht in direktem Zusammenhang mit PPP stehen. In diesem Kapitel wird erklärt, welche Planungsaufgaben für allgemeine PPP-Verbindungen, die Authentifizierung und für PPPoE durchzuführen sind.

In den Kapiteln, die nach Kapitel 16, „PLanen einer PPP-Verbindung (Aufgaben)“ folgen, werden Beispielkonfigurationen verwendet, um zu erläutern, wie eine bestimmte Verbindung eingerichtet wird. Diese Beispielkonfigurationen werden in diesem Kapitel vorgestellt.

Folgende Themen werden behandelt:

- „Planen einer PPP-Einwahlverbindung“ auf Seite 438
- „Planen einer Standleitungsverbindung“ auf Seite 442
- „Planen der Authentifizierung zur Verwendung einer Verbindung“ auf Seite 445
- „Planen der DSL-Unterstützung über einen PPPoE-Tunnel“ auf Seite 450

PPP-Gesamtplanung (Übersicht der Schritte)

PPP erfordert die Planung von Aufgaben, bevor Sie mit dem Einrichten der Verbindung beginnen können. Wenn Sie PPPoE-Tunneling verwenden möchten, müssen Sie zuerst die PPP-Verbindung und dann das Tunneling einrichten. In der folgenden Tabelle werden die umfangreichen Planungsaufgaben aufgelistet, die in diesem Kapitel erläutert werden. Eventuell müssen Sie nur die allgemeine Aufgabe für die Verbindung verwenden, die konfiguriert werden soll. Es kann aber auch sein, dass Sie die Aufgabe für die Verbindung, die Authentifizierung und eventuell auch für PPPoE benötigen.

TABELLE 16–1 Übersicht der Schritte für die PPP-Planung

Aufgabe	Beschreibung	Siehe
Planen einer PPP-Wählverbindung	Sammeln von Informationen, die für das Einrichten eines Hinauswahlrechners oder eines Einwahlservers benötigt werden	„Planen einer PPP-Einwahlverbindung“ auf Seite 438
Planen einer Standleitungsverbindung	Sammeln von Informationen, die für das Einrichten eines Clients an einer Standleitung benötigt werden	„Planen einer Standleitungsverbindung“ auf Seite 442
Planung der Authentifizierung für die PPP-Verbindung	Sammeln von Informationen, die zum Konfigurieren der PAP- oder CHAP-Authentifizierung für die PPP-Verbindung benötigt werden	„Planen der Authentifizierung zur Verwendung einer Verbindung“ auf Seite 445
Planen eines PPPoE-Tunnel	Sammeln von Informationen, die für das Einrichten eines PPPoE-Tunnels benötigt werden, über den eine PPP-Verbindung laufen kann	„Planen der DSL-Unterstützung über einen PPPoE-Tunnel“ auf Seite 450

Planen einer PPP-Einwahlverbindung

Wählverbindungen sind die gebräuchlichsten PPP-Verbindungen. Dieser Abschnitt enthält folgende Informationen:

- Planungsinformationen für eine Wählverbindung
- Eine Erklärung der Beispielverbindung (siehe Kapitel 17, „Einrichten einer PPP-Einwahlverbindung (Aufgaben)“)

Normalerweise wird der Rechner nur an einem Ende der PPP-Wählverbindung konfiguriert, d. h. am Ende des Hinauswahlrechners oder des Einwahlservers. Eine Einführung zum Thema PPP-Anwahl finden Sie unter „PPP-Einwahlverbindung – Übersicht“ auf Seite 425.

Vor dem Einrichten des Hinauswahlrechners

Bevor Sie einen Hinauswahlrechner konfigurieren, sammeln Sie die in der folgenden Tabelle aufgeführten Informationen.

Hinweis – Die in diesem Abschnitt aufgeführten Planungsinformationen schließen keine Informationen ein, die über die Authentifizierung oder PPPoE gesammelt werden können. Weitere Informationen zur Planung der Authentifizierung finden Sie unter „Planen der Authentifizierung zur Verwendung einer Verbindung“ auf Seite 445. Informationen zur PPPoE-Planung finden Sie unter „Planen der DSL-Unterstützung über einen PPPoE-Tunnel“ auf Seite 450.

TABELLE 16–2 Informationen für einen Hinauswahlrechner

Informationen	Aktion
Maximale Modemgeschwindigkeit	Informieren Sie sich in der Dokumentation des Modemherstellers.
Modemverbindungsbefehle (AT-Befehle)	Entnehmen Sie die erforderlichen Informationen der Dokumentation des Modemherstellers.
Name, der für den Einwahlserver am anderen Ende der Verbindung zu verwenden ist	Erstellen Sie einen Namen, mit dem Sie den Einwahlserver identifizieren können.
Anmeldesequenz, die vom Einwahlserver verlangt wird	Wenden Sie sich an den Administrator des Einwahlservers, oder ziehen Sie die ISP-Dokumentation heran, wenn sich der Einwahlserver am Standort des ISP befindet.

Vor dem Einrichten des Einwahlservers

Bevor Sie einen Einwahlserver konfigurieren, sammeln Sie die in der folgenden Tabelle aufgeführten Informationen.

Hinweis – Die in diesem Abschnitt aufgeführten Planungsinformationen schließen keine Informationen ein, die über die Authentifizierung oder PPPoE gesammelt werden können. Weitere Informationen zur Planung der Authentifizierung finden Sie unter „Planen der Authentifizierung zur Verwendung einer Verbindung“ auf Seite 445. Informationen zur PPPoE-Planung finden Sie unter „Planen der DSL-Unterstützung über einen PPPoE-Tunnel“ auf Seite 450.

TABELLE 16–3 Informationen für einen Einwahlserver

Informationen	Aktion
Maximale Modemgeschwindigkeit	Entnehmen Sie die erforderlichen Informationen der Dokumentation des Modemherstellers.
Benutzernamen von Personen, denen erlaubt ist, den Einwahlserver aufzurufen	Stellen Sie die Namen von potenziellen Benutzern bereit, bevor Sie die Home-Verzeichnisse dieser Benutzer einrichten (siehe „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466).

TABELLE 16–3 Informationen für einen Einwahlserver *(Fortsetzung)*

Informationen	Aktion
Dedizierte IP-Adresse für die PPP-Kommunikation	Stellen Sie eine Adresse der Person in Ihrem Unternehmen bereit, die verantwortlich für das Delegieren von IP-Adressen ist.

Beispiel einer Konfiguration für eine PPP-Einwahlverbindung

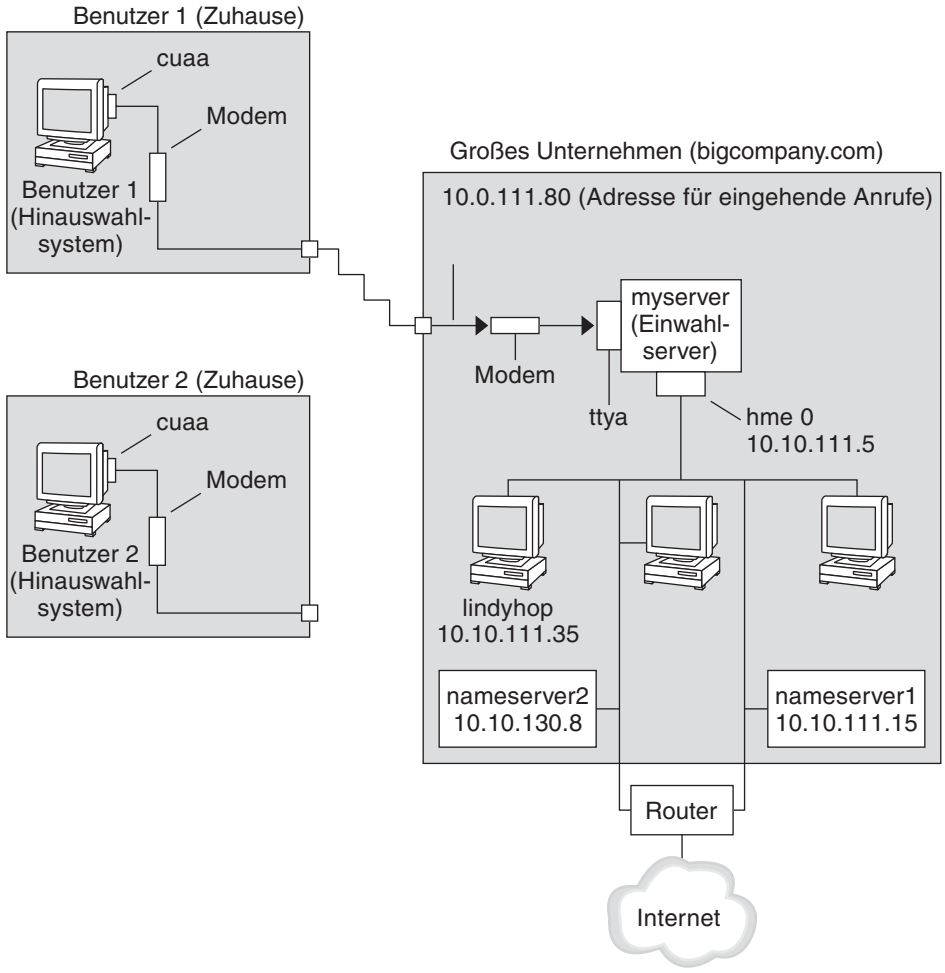
Durch Ausführen der Aufgaben, die in Kapitel 17, „Einrichten einer PPP-Einwahlverbindung (Aufgaben)“ beschrieben sind, wird den Mitarbeitern eines kleinen Unternehmens ermöglicht, an einigen Tagen in der Woche zu Hause zu arbeiten. Auf einigen Heimrechnern der Mitarbeiter muss das Betriebssystem Solaris installiert werden. Die Mitarbeiter müssen sich von Ihren Heimrechnern aus beim Intranet des Unternehmens anmelden können.

In den Aufgaben wird beschrieben, wie eine einfache Wählverbindung mit folgenden Funktionen eingerichtet wird:

- Die *Hinauswahlrechner* befinden sich in den Wohnungen der Mitarbeiter, die das Intranet des Unternehmens aufrufen müssen.
- Der *Einwahlserver* ist ein Rechner im Unternehmensintranet, der eingehende Aufrufe von Mitarbeitern empfängt.
- Für die Authentifizierung des Hinauswahlrechners wird eine UNIX-basierte Anmeldung verwendet. Die Sicherheitsrichtlinien des Unternehmens verlangen keine strengeren Solaris PPP 4.0-Authentifizierungsverfahren.

In den folgenden Abschnitten wird die Verbindung gezeigt, die anhand der in Kapitel 17, „Einrichten einer PPP-Einwahlverbindung (Aufgaben)“ beschriebenen Schritte eingerichtet wurde.

ABBILDUNG 16–1 Einwahlverbindung – Beispiel



Diese Abbildung zeigt einen Remote-Host, dessen Modem verwendet wird, um über Telefonleitungen das Intranet von Big Company anzuwählen. Ein anderer Host führt die Hinauswahl zu Big Company aus, ist aber derzeit inaktiv. Die Anrufe von Remote-Benutzern werden in der Reihenfolge beantwortet, in der sie vom Modem empfangen werden, das an den Einwahlserver von Big Company angeschlossen ist. Zwischen den Peers wird eine PPP-Verbindung hergestellt. Der Hinauswahlrechner kann sich dann per Remote-Zugriff bei einem Hostrechner im Intranet anmelden.

Weitere Informationen zur PPP-Anwahl

Relevante Informationen finden Sie unter:

- Einrichten eines Hinauswahlrechners (siehe Tabelle 17–2)
- Einrichten eines Einwahlrechners (siehe Tabelle 17–3)
- Übersicht zu Wählverbindungen (siehe „PPP-Einwahlverbindung – Übersicht“ auf Seite 425)
- Ausführliche Informationen zu PPP-Dateien und -Befehlen (siehe „Verwenden von PPP-Optionen in Dateien und in der Befehlszeile“ auf Seite 525)

Planen einer Standleitungsverbindung

Zum Einrichten einer Standleitungsverbindung muss ein Peer an einem Ende eines geschalteten oder nicht geschalteten Services konfiguriert werden, der von einem Provider gemietet ist.

Dieser Abschnitt enthält folgende Informationen:

- Planungsinformationen für eine Standleitungsverbindung
- Erklärung der in Abbildung 16–2 dargestellten Beispielverbindung

Eine Einführung zu Standleitungsverbindungen finden Sie unter „PPP-Standleitung – Übersicht“ auf Seite 429. Aufgaben zum Einrichten der Standleitung finden Sie in Kapitel 18, „Einrichten einer PPP-Standleitungsverbindung (Aufgaben)“.

Vor dem Einrichten der Standleitungsverbindung

Wenn Ihr Unternehmen eine Standleitungsverbindung von einem Netzbetreiber mietet, müssen Sie normalerweise nur das System an Ihrem Ende der Verbindung konfigurieren. Der Peer am anderen Ende der Verbindung wird von einem anderen Administrator verwaltet. Diese Person kann ein Systemadministrator an einem Remote-Standort in Ihrem Unternehmen oder ein Systemadministrator bei einem ISP sein.

Für eine Standleitungsverbindung benötigte Hardware

Zusätzlich zum Verbindungsmedium wird für Ihr Ende der Verbindung folgende Hardware benötigt:

- Eine synchrone Schnittstelle für Ihr System
- Ein synchrones Gerät (CSU/DSU)
- Ihr System

Zu den Teilnehmerendgeräten, die manche Netzbetreiber bereitstellen, gehören ein Router, eine synchrone Schnittstelle und ein CSU/DSU. Der Bedarf an Geräten kann jedoch variieren,

was vom Provider und den allgemeinen Vorschriften abhängt, die für Ihr Gebietsschema gelten. Der Netzbetreiber kann Ihnen Informationen zum benötigten Gerät geben, wenn dieses Gerät nicht zusammen mit der Standleitung bereitgestellt wird.

Informationen, die für die Standleitungsverbindung zu sammeln sind

Bevor Sie den lokalen Peer konfigurieren, müssen Sie die in der folgenden Tabelle aufgeführten Informationen sammeln.

TABELLE 16–4 Planen einer Standleitungsverbindung

Informationen	Aktion
Gerätename der Schnittstelle	Lesen Sie dazu die Dokumentation der Schnittstellenkarte.
Konfigurationsanweisungen für die synchrone Schnittstellenkarte	Lesen Sie dazu die Dokumentation der Schnittstellenkarte. Sie benötigen dieses Informationen, um die HSI/P-Schnittstelle zu konfigurieren. Eventuell müssen Sie keine anderen Schnittstellenkarten konfigurieren.
(Optional) IP-Adresse des Remote-Peer	Lesen Sie dazu die Dokumentation des Serviceproviders. Sie können sich auch an den Systemadministrator des Remote-Peers wenden. Diese Informationen werden nur dann benötigt, wenn die IP-Adresse zwischen den beiden Peers ausgehandelt wird.
(Optional) Name des Remote-Peers	Lesen Sie dazu die Dokumentation des Serviceproviders. Sie können sich auch an den Systemadministrator des Remote-Peers wenden.
(Optional) Geschwindigkeit der Verbindung	Lesen Sie dazu die Dokumentation des Serviceproviders. Sie können sich auch an den Systemadministrator des Remote-Peers wenden.
(Optional) Komprimierung, die vom Remote-Peer verwendet wird	Lesen Sie dazu die Dokumentation des Serviceproviders. Sie können sich auch an den Systemadministrator des Remote-Peers wenden.

Beispielkonfiguration für eine Standleitungsverbindung

Die in Kapitel 18, „Einrichten einer PPP-Standleitungsverbindung (Aufgaben)“ beschriebenen Aufgaben zeigen, wie für die Mitarbeiter eines mittelgroßen Unternehmens (LocalCorp) ein Internetzugang bereitgestellt wird. Derzeit sind die Computer der Mitarbeiter über ein privates Unternehmensintranet verbunden.

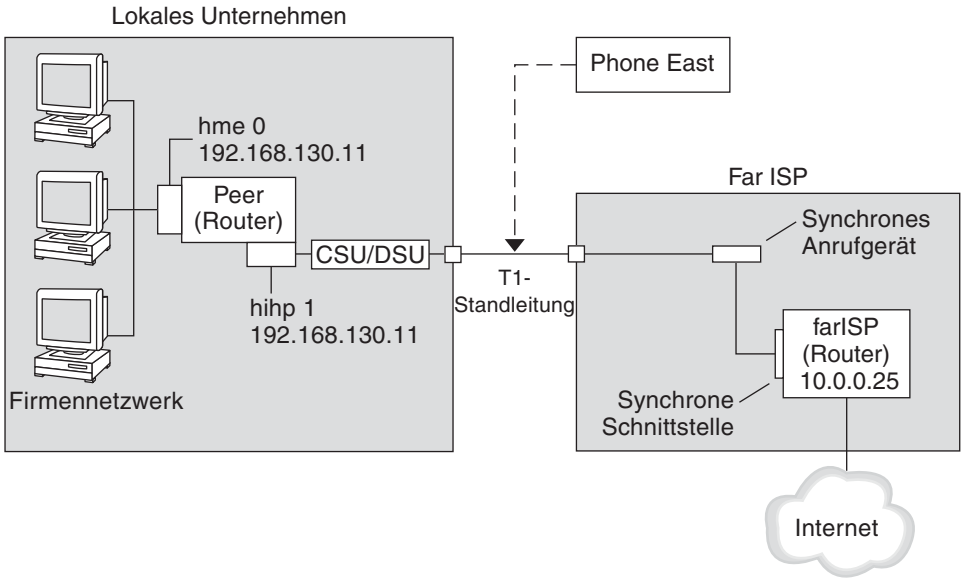
LocalCorp benötigt zügige Transaktionen und Zugriff auf viele Ressourcen im Internet. Das Unternehmen schließt einen Vertrag mit Far ISP ab, einem Serviceprovider, wodurch LocalCorp eine eigene Standleitung zu Far ISP einrichten kann. Anschließend mietet

LocalCorp eine T1-Leitung von Phone East, einer Telefongesellschaft. Phone East richtet die Standleitung zwischen LocalCorp und Far ISP ein. Dann stellt Phone East ein CSU/DSU bereit, das bereits für LocalCorp konfiguriert ist.

In den Aufgaben wird die Einrichtung einer Standleitungsverbindung mit folgenden Merkmalen beschrieben:

- LocalCorp hat ein System als Gateway-Router eingerichtet, der Pakete über die Standleitung an Hosts im Internet weiterleitet.
- Far ISP hat zudem einen Peer als Router eingerichtet, an den Standleitungen des Kunden angeschlossen sind.

ABBILDUNG 16–2 Beispiel einer Standleitungskonfiguration



Die Abbildung zeigt einen Router, der für PPP bei LocalCorp eingerichtet ist. Der Router verbindet das Unternehmensintranet über die `hme0`-Schnittstelle. Die zweite Verbindung mit dem digitalen CSU/DSU-Gerät wird über die HSI/P-Schnittstelle (hihp1) des Rechners hergestellt. Das CSU/DSU verbindet dann die installierte Standleitung. Der Administrator von LocalCorp konfiguriert die HSI/P-Schnittstelle und die PPP-Dateien. Dann gibt der Administrator `/etc/init.d/pppd` ein, um die Verbindung zwischen LocalCorp und Far ISP zu initiieren.

Weitere Informationen zu Standleitungen

Relevante Informationen finden Sie unter:

- Kapitel 18, „Einrichten einer PPP-Standleitungsverbindung (Aufgaben)“
- „PPP-Standleitung – Übersicht“ auf Seite 429

Planen der Authentifizierung zur Verwendung einer Verbindung

Dieser Abschnitt enthält Planungsinformationen für die Authentifizierung zur Verwendung einer PPP-Verbindung. Kapitel 19, „Einrichten der PPP-Authentifizierung (Aufgaben)“ enthält Aufgaben für die Implementierung der PPP-Authentifizierung an Ihrem Standort.

PPP bietet zwei Arten der Authentifizierung: die unter „PAP (Password Authentication Protocol)“ auf Seite 549 beschriebene PAP-Authentifizierung und die unter „CHAP (Challenge-Handshake Authentication Protocol)“ auf Seite 552 beschriebene CHAP-Authentifizierung.

Bevor Sie die Authentifizierung für eine Verbindung einrichten, müssen Sie entscheiden, welches Authentifizierungsprotokoll am besten die Sicherheitsrichtlinien Ihres Standorts erfüllt. Danach richten Sie die Geheimnisdatei und die PPP-Konfigurationsdateien für die Einwahlrechner, die Hinauswahlrechner oder beide Rechner ein. Weitere Informationen zur Wahl des richtigen Authentifizierungsprotokolls für Ihren Standort finden Sie unter „Warum die PPP-Authentifizierung verwendet werden sollte“ auf Seite 433.

Dieser Abschnitt enthält folgende Informationen:

- Planungsinformationen für die PAP- und CHAP-Authentifizierung
- Erklärungen der Beispielszenarios für die Authentifizierung, die in Abbildung 16–3 und Abbildung 16–4 dargestellt werden

Aufgaben zum Einrichten der Authentifizierung finden Sie in Kapitel 19, „Einrichten der PPP-Authentifizierung (Aufgaben)“.

Vor dem Einrichten der PPP-Authentifizierung

Das Einrichten der Authentifizierung an Ihrem Standort sollte ein integraler Bestandteil Ihrer PPP-Gesamtstrategie sein. Vor der Implementierung der Authentifizierung sollten Sie die Hardware installieren, die Software konfigurieren und die Verbindung testen.

TABELLE 16–5 Voraussetzungen zum Konfigurieren der Authentifizierung

Informationen	Siehe
Aufgaben zum Konfigurieren einer Wählverbindung	Kapitel 17, „Einrichten einer PPP-Einwahlverbindung (Aufgaben)“.
Aufgaben zum Testen der Verbindung	Kapitel 21, „Beheben von allgemeinen PPP-Problemen (Aufgaben)“.
Sicherheitsanforderungen für Ihren Standort	Sicherheitsrichtlinien Ihres Unternehmens. Wenn keine Sicherheitsrichtlinien vorhanden sind, haben Sie beim Einrichten der PPP-Authentifizierung die Gelegenheit, Sicherheitsrichtlinien zu erstellen.
Informationen zum sinnvollen Einsatz von PAP oder CHAP	„Warum die PPP-Authentifizierung verwendet werden sollte“ auf Seite 433. Weitere Informationen zu diesen Protokollen finden Sie unter „Authentifizieren von Anrufern“ auf Seite 549.

Beispiele für PPP-Authentifizierungskonfigurationen

Dieser Abschnitt enthält Beispiele für Authentifizierungsszenarios, die in den unter Kapitel 19, „Einrichten der PPP-Authentifizierung (Aufgaben)“ beschriebenen Verfahren verwendet werden.

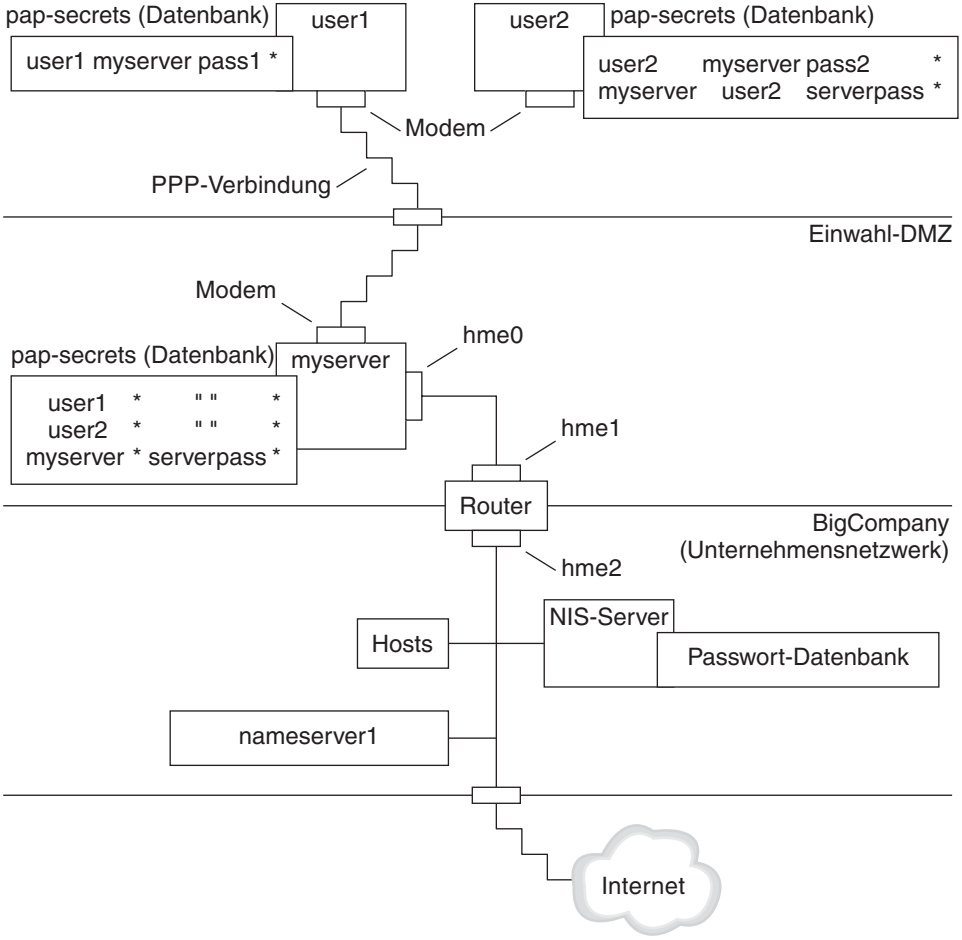
- „Beispielkonfiguration mit PAP-Authentifizierung“ auf Seite 446
- „Beispiel einer Konfiguration mit CHAP-Authentifizierung“ auf Seite 448

Beispielkonfiguration mit PAP-Authentifizierung

Die unter „Konfigurieren der PAP-Authentifizierung“ auf Seite 478 beschriebenen Aufgaben zeigen, wie die PAP-Authentifizierung über die PPP-Verbindung eingerichtet wird. In den Verfahren wird ein PAP-Beispielszenario für das fiktive Unternehmen "Big Company" verwendet (siehe „Beispiel einer Konfiguration für eine PPP-Einwahlverbindung“ auf Seite 440).

Big Company beabsichtigt, Heimarbeitsplätze für seine Benutzer einzurichten. Die Systemadministratoren benötigen eine sichere Lösung für die seriellen Verbindungen mit dem Einwahlserver. In der Vergangenheit wurden bei Big Company NIS-Passwortdatenbanken mit UNIX-basierter Anmeldung verwendet. Die Systemadministratoren benötigen ein UNIX-basiertes Authentifizierungsschema für Anrufe, die über eine PPP-Verbindung in das Netzwerk gelangen. Aus diesen Gründen implementieren die Administratoren das folgende Szenario mit PAP-Authentifizierung.

ABBILDUNG 16–3 Beispiel eines PAP-Authentifizierungsszenarios (Heimarbeitsplatz)



Die Systemadministratoren erstellen eine dedizierte Einwahl-DMZ, die vom übrigen Teil des Unternehmensnetzwerks durch einen Router getrennt ist. Der Begriff "DMZ" stammt vom militärischen Begriff "entmilitarisierte Zone" (demilitarized zone) ab. Die DMZ ist ein isoliertes Netzwerk für Sicherheitszwecke. In der DMZ befinden sich Ressourcen, die ein Unternehmen für die Öffentlichkeit bereitstellt, beispielsweise Webserver, anonyme FTP-Server, Datenbanken und Modemserver. Netzwerkentwickler platzieren die DMZ oft zwischen einer Firewall und dem Internetzugang eines Unternehmens.

Die einzigen Geräte in der DMZ, die in Abbildung 16–3 dargestellt sind, sind der Einwahlserver `myserver` und der Router. Der Einwahlserver verlangt von den aufrufenden Programmen, PAP-Berechtigungsnachweise wie Benutzernamen und Passwörter anzugeben, wenn die Verbindung eingerichtet wird. Außerdem verwendet der Einwahlserver die Anmeldeoption (`login`) von PAP. Aus diesem Grund müssen die PAP-Benutzernamen und -Passwörter des

Anrufers genau mit den entsprechenden UNIX-Benutzernamen und -Passwörtern übereinstimmen, die in der Passwortdatenbank des Einwahlserver enthalten sind.

Nach der Herstellung der PPP-Verbindung werden die Pakete des Anrufers an den Router weitergeleitet. Vom Router werden die Daten an das Ziel im Unternehmensnetzwerk oder im Internet weitergeleitet.

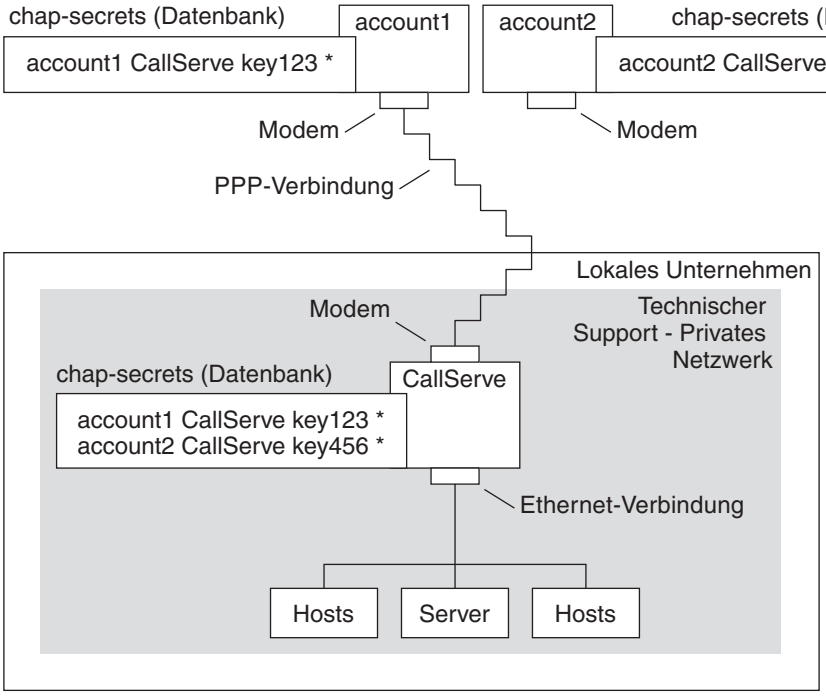
Beispiel einer Konfiguration mit CHAP-Authentifizierung

Die unter „Konfigurieren der CHAP-Authentifizierung “ auf Seite 486 beschriebenen Aufgaben zeigen, wie die CHAP-Authentifizierung eingerichtet wird. In den Verfahren wird ein CHAP-Szenario als Beispiel für das fiktive Unternehmen LocalCorp verwendet, das unter „Beispielkonfiguration für eine Standleitungsverbindung“ auf Seite 443 vorgestellt wurde.

LocalCorp sorgt für Internetkonnektivität über eine Standleitung mit einem ISP. Der technische Support von LocalCorp ruft starken Netzwerkverkehr hervor. Darum benötigt der technische Support ein eigenes, isoliertes privates Netzwerk. Die Außendiensttechniker der Abteilung sind viel auf Reisen und müssen von Remote-Standorten aus auf das Netzwerk des technischen Supports zugreifen, um an Informationen zu gelangen, die zur Lösung von Problemen dienen. Um die in der Datenbank des Netzwerks enthaltenen vertraulichen Informationen zu schützen, müssen Remote-Anrufer authentifiziert werden, damit sie sich anmelden können.

Aus diesen Gründen implementieren die Systemadministratoren das folgende CHAP-Authentifizierungsszenario für eine PPP-Anwahlkonfiguration.

ABBILDUNG 16–4 Beispiel eines CHAP-Authentifizierungsszenarios (Anwahl eines privaten Netzwerks)



Die einzige Verbindung des Netzwerks des technischen Supports zur Außenwelt ist die serielle Verbindung mit dem Verbindungsende des Einwahlservers. Die Systemadministratoren konfigurieren die Laptops aller Außendienstmitarbeiter für PPP mit CHAP-Sicherheit einschließlich CHAP-Geheimnis. Die CHAP-Geheimnisdatenbank auf dem Einwahlserver enthält die CHAP-Berechtigungsnachweise für alle Rechner, denen erlaubt ist, das Netzwerk des technischen Supports aufzurufen.

Weitere Informationen zur Authentifizierung

Wählen Sie eines der folgenden Verfahren:

- „Konfigurieren der PAP-Authentifizierung“ auf Seite 478
- „Konfigurieren der CHAP-Authentifizierung “ auf Seite 486
- „Authentifizieren von Anrufern“ auf Seite 549 und das Verfahren auf der Manpage `pppd(1M)`

Planen der DSL-Unterstützung über einen PPPoE-Tunnel

Manche DSL-Provider verlangen von Ihnen, PPPoE-Tunneling für Ihren Standort einzurichten, damit PPP über die DSL-Leitungen und Hochgeschwindigkeitsnetzwerke des Providers ausgeführt werden kann. Eine Übersicht zu PPPoE finden Sie unter „Unterstützung für DSL-Benutzer durch PPPoE“ auf Seite 433.

Zu einem PPPoE-Tunnel gehören drei Teilnehmer: ein Konsument, eine Telefongesellschaft und ein ISP. Entweder konfigurieren Sie PPPoE für Konsumenten wie beispielsweise PPPoE-Clients in Ihrem Unternehmen oder Konsumenten in Privathaushalten, oder Sie konfigurieren PPPoE auf einem Server bei einem ISP.

Dieser Abschnitt enthält Planungsinformationen für das Ausführen von PPPoE sowohl auf Clients als auch auf Zugangsservern. Folgende Themen werden behandelt:

- Planungsinformationen für den PPPoE-Host und den Zugangsserver
- Erklärung des unter „Beispiel einer Konfiguration für einen PPPoE-Tunnel“ auf Seite 452 vorgestellten PPPoE-Szenarios

Aufgaben zum Einrichten eines PPPoE-Tunnels finden Sie in Kapitel 20, „Einrichten eines PPPoE-Tunnels (Aufgaben)“.

Vor dem Einrichten eines PPPoE-Tunnels

Die Maßnahmen vor der Konfiguration hängen davon ab, ob Sie die Clientseite oder die Serverseite des Tunnels konfigurieren. In jedem Fall müssen Sie oder Ihr Unternehmen einen Vertrag mit einer Telefongesellschaft abschließen. Die Telefongesellschaft stellt die DSL-Leitungen für Clients, eine Form der Überbrückung und möglicherweise eine ATM-Leitung für Zugangsserver bereit. In den meisten Verträgen ist festgelegt, dass die Telefongesellschaft ihre Geräte in dem betreffenden Unternehmen installiert.

Vor dem Konfigurieren eines PPPoE-Clients

Für die PPPoE-Clientimplementierungen werden normalerweise folgende Geräte verwendet:

- PC oder ein anderer Rechner, der von einer Person verwendet wird
- DSL-Modem, das normalerweise von der Telefongesellschaft oder dem ISP installiert wird
- (Optional) ein Hub, wenn mehrere Clients verwendet werden, beispielsweise bei DSL-Firmenkunden
- (Optional) ein Splitter, der normalerweise vom Provider installiert wird

Es sind viele verschiedene DSL-Konfigurationen möglich, was vom Benutzer oder von den unternehmensspezfischen Erfordernissen und den vom Provider angebotenen Services abhängt.

TABELLE 16–6 Planen der PPPoE-Clients

Informationen	Aktion
Wenn Sie einen Heim-PPPoE-Client für eine Person oder sich selbst einrichten, sollten Sie sich alle Informationen zum Einrichten beschaffen, die nicht in der PPPoE-Dokumentation enthalten sind.	Fordern Sie bei der Telefongesellschaft oder dem ISP Material zu sämtlichen Einrichtungsverfahren an.
Wenn Sie PPPoE-Clients in einem Unternehmen einrichten, sammeln Sie die Namen der Benutzer, denen PPPoE-Clientsysteme zugewiesen werden. Wenn Sie Remote-PPPoE-Clients konfigurieren, müssen Sie unter Umständen den Benutzern die Informationen bereitstellen, die den Einsatz von DSL-Geräten in Privathaushalten betreffen.	Fordern Sie beim Management Ihrer Firma eine Liste der autorisierten Benutzer an.
Finden Sie heraus, welche Schnittstellen auf dem PPPoE-Client verfügbar sind.	Führen Sie auf jedem Rechner den Befehl `ifconfig -a` für Schnittstellennamen aus.
(Optional) Stellen Sie das Passwort für den PPPoE-Client bereit.	Fragen Sie die Benutzer, welche Passwörter sie verwenden möchten. Sie können die Passwörter den Benutzern auch zuweisen. Beachten Sie, dass dieses Passwort für die Verbindungsauthentifizierung verwendet wird, nicht aber für die UNIX-Anmeldung.

Vor dem Konfigurieren eines PPPoE-Servers

Die Planung für einen PPPoE-Zugangsserver erfordert eine Zusammenarbeit mit der Telefongesellschaft, die ihr Datenservicetnetz mit Ihrem System verbindet. Die Telefongesellschaft installiert die Leitungen, meist ATM-Leitungen, an Ihrem Standort und stellt eine Form der Überbrückung zu Ihrem Zugangsserver bereit. Sie müssen die Ethernet-Schnittstellen konfigurieren, um Zugang zu den Services zu erhalten, die von Ihrem Unternehmen bereitgestellt werden. Es müssen beispielsweise Schnittstellen für den Internetzugang sowie Ethernet-Schnittstellen für die Brücke der Telefongesellschaft konfiguriert werden.

TABELLE 16–7 Planung für einen PPPoE-Zugangsserver

Informationen	Aktion
Schnittstellen, die für Leitungen vom Datenservicenetz verwendet werden	Führen Sie den Befehl `ifconfig -a` aus, um die Schnittstellen zu identifizieren.
Services, die über den PPPoE-Server bereitgestellt werden	Erkundigen Sie sich beim Management und den Netzwerkplanern nach ihren Erfordernissen, und bitten Sie sie um Vorschläge.
(Optional) Services für die Konsumenten	Erkundigen Sie sich beim Management und den Netzwerkplanern nach ihren Erfordernissen, und bitten Sie sie um Vorschläge.

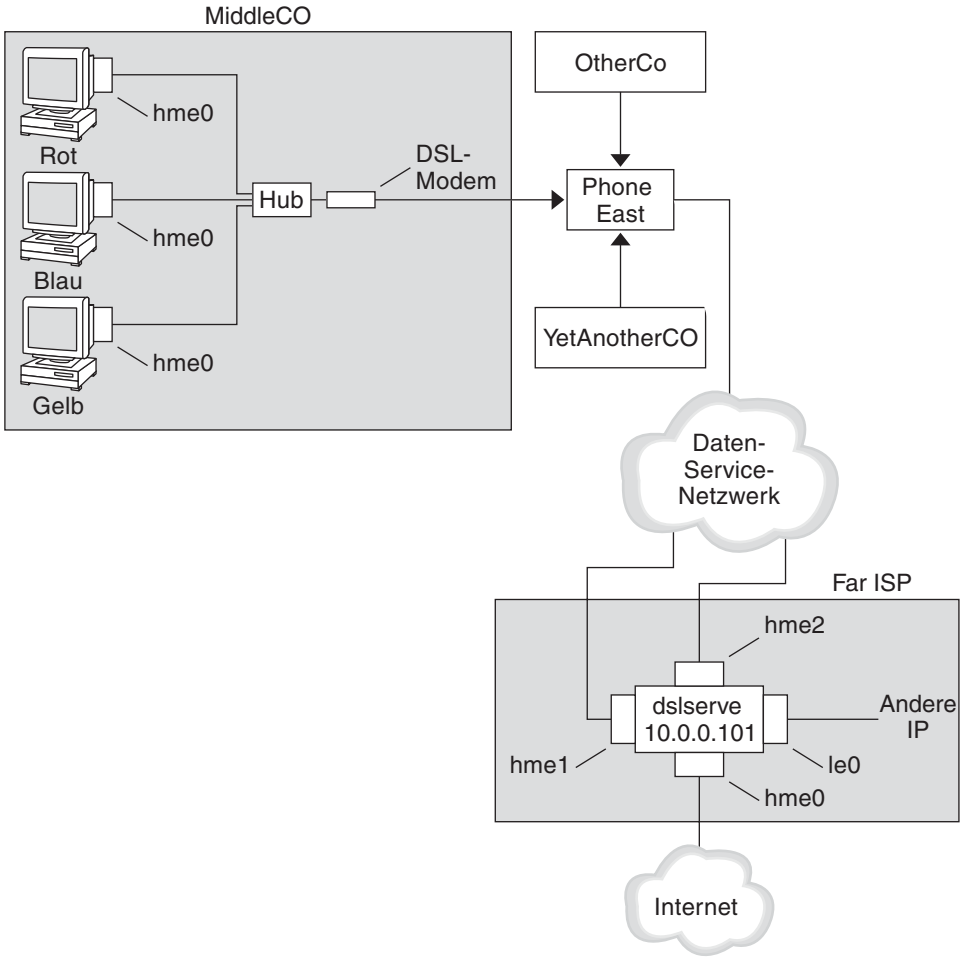
TABELLE 16–7 Planung für einen PPPoE-Zugangsserver *(Fortsetzung)*

Informationen	Aktion
(Optional) Hostnamen und Passwörter für Remote-Clients	Fragen Sie die Netzwerkplaner und andere Personen an Ihrem Standort, die für Vertragsverhandlungen zuständig ist. Die Hostnamen und Passwörter werden für die PAP- oder CHAP-Authentifizierung verwendet, nicht aber für die UNIX-Anmeldung.

Beispiel einer Konfiguration für einen PPPoE-Tunnel

Das in diesem Abschnitt enthaltene Beispiel für einen PPPoE-Tunnel dient zur Erläuterung der Aufgaben, die in Kapitel 20, „Einrichten eines PPPoE-Tunnels (Aufgaben)“ aufgeführt sind. Obwohl die Abbildung den Tunnel und alle Teilnehmer zeigt, verwalten Sie nur ein Ende, entweder die Clientseite oder die Serverseite.

ABBILDUNG 16–5 Beispiel eines PPPoE-Tunnels



In diesem Beispiel beabsichtigt MiddleCo, für seine Mitarbeiter einen Hochgeschwindigkeitsinternetzugang bereitzustellen. MiddleCo kauft ein DSL-Paket von Phone East, und Phone East schließt einen Vertrag mit dem Serviceprovider Far ISP. Far ISP bietet Kunden, die DSL von Phone East kaufen, den Internetzugang und andere IP-Services an.

Beispiel einer PPPoE-Clientkonfiguration

MiddleCo kauft ein Paket von Phone East, und Phone East stellt eine DSL-Leitung für den Standort bereit. Das Paket enthält eine dedizierte, authentifizierte Verbindung mit dem ISP für die PPPoE-Clients von MiddleCo. Der Systemadministrator verkabelt die potenziellen PPPoE-Clients mit einem Hub. Die Techniker von Phone East verkabeln den Hub mit ihren DSL-Geräten.

Beispiel eines PPPoE-Server-Konfiguration

Entsprechend der geschäftlichen Vereinbarung, die FarISP mit Phone East getroffen hat, konfiguriert der Systemadministrator bei FarISP den Zugangsserver `dslserve`. Dieser Server verfügt über die folgenden vier Schnittstellen:

- `eri0` – primäre Netzwerkschnittstelle zur Verbindung mit dem lokalen Netzwerk
- `hme0` – Schnittstelle, über die FarISP für seine Kunden den Internetservice bereitstellt
- `hme1` – Schnittstelle, für die MiddleCo einen Vertrag abgeschlossen hat, der sich auf authentifizierte PPPoE-Tunnel bezieht
- `hme2` – Schnittstelle, für die andere Kunden einen Vertrag abgeschlossen haben, der sich auf die PPPoE-Tunnel dieser Kunden bezieht

Weitere Informationen zu PPPoE

Wählen Sie eines der folgenden Verfahren:

- „Einrichten des PPPoE-Clients“ auf Seite 496.
- „Einrichten eines PPPoE-Zugangsservers“ auf Seite 500.
- „Erstellen von PPPoE-Tunneln für DSL-Unterstützung“ auf Seite 558 und die Manpages `pppoed`(1M), `pppoec`(1M) und `sppptun`(1M).

◆ ◆ ◆ KAPITEL 17

Einrichten einer PPP-Einwahlverbindung (Aufgaben)

In diesem Kapitel werden die Aufgaben beschrieben, die zum Konfigurieren der gebräuchlichsten PPP-Verbindung, der Wählverbindung, durchgeführt werden müssen. Folgende Themen werden behandelt:

- „Konfigurieren des Hinauswahlrechners“ auf Seite 456
- „Konfigurieren des Einwahlservers“ auf Seite 463
- „Aufrufen des Einwahlservers“ auf Seite 469

Wichtige Aufgaben zum Einrichten der PPP-Einwahlverbindung (Übersicht der Schritte)

Sie richten eine PPP-Einwahlverbindung ein, indem Sie Modems konfigurieren, Dateien von Netzwerkdatenbanken modifizieren und die PPP-Konfigurationsdateien modifizieren, die in Tabelle 22–1 beschrieben sind.

In der folgenden Tabelle werden die wichtigsten Aufgaben zum Konfigurieren beider Seiten einer PPP-Einwahlverbindung aufgelistet. Normalerweise wird nur eine Seite der Verbindung konfiguriert, entweder der Hinauswahlrechner oder der Einwahlserver.

TABELLE 17–1 Übersicht der Schritte zum Einrichten der PPP-Wählverbindung

Aufgabe	Beschreibung	Siehe
1. Sammeln von Informationen vor der Konfiguration	Sammeln Sie vor dem Einrichten der Verbindung die benötigten Daten, beispielsweise Peer-Hostnamen, Zieltelefonnummern und Modemgeschwindigkeit.	„Planen einer PPP-Einwahlverbindung“ auf Seite 438
2. Konfigurieren des Hinauswahlrechners	Richten Sie PPP auf dem Rechner ein, der für Aufrufe die Verbindung verwendet.	Tabelle 17–2

TABELLE 17–1 Übersicht der Schritte zum Einrichten der PPP-Wählverbindung *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
3. Konfigurieren des Einwahlservers	Richten Sie PPP auf dem Rechner ein, der eingehende Anrufe empfängt.	Tabelle 17–3
4. Aufrufen des Einwahlservers	Geben Sie den Befehl `pppd` ein, um die Kommunikation zu initiieren.	„So rufen Sie den Einwahlserver auf“ auf Seite 469

Konfigurieren des Hinauswahlrechners

Die Aufgaben in diesem Abschnitt zeigen, wie ein Hinauswahlrechner konfiguriert wird. Als Beispiel dient das in Abbildung 16–1 dargestellte Home-Einwahlszenario. Sie können die Aufgaben in Ihrer Firma ausführen, bevor Sie den Rechner an einen potenziellen Benutzer weitergeben. Auch können Sie erfahrene Benutzer instruieren, damit diese ihre Heimrechner selbst einrichten können. Jede Person, die einen Hinauswahlrechner einrichtet, muss über Root-Berechtigungen für den betreffenden Rechner verfügen.

Aufgaben zum Konfigurieren des Hinauswahlrechners (Übersicht der Schritte)

TABELLE 17–2 Übersicht der Schritte zum Einrichten des Hinauswahlrechners

Aufgabe	Beschreibung	Siehe
1. Sammeln von Informationen vor der Konfiguration	Sammeln Sie vor dem Einrichten der Verbindung die benötigten Daten, beispielsweise Peer-Hostnamen, Zieltelefonnummern und Modemgeschwindigkeit.	„Planen einer PPP-Einwahlverbindung“ auf Seite 438
2. Konfigurieren des Modems und des seriellen Ports	Richten Sie das Modem und den seriellen Port ein.	„So konfigurieren Sie das Modem und den seriellen Port (Hinauswahlrechner)“ auf Seite 458
3. Konfigurieren der Kommunikation über eine serielle Verbindung	Konfigurieren Sie die Eigenschaften der Kommunikation über eine serielle Verbindung.	„So definieren Sie die Kommunikation über die serielle Verbindung“ auf Seite 460
4. Definieren der Kommunikation zwischen Hinauswahlrechner und Peer	Sammeln Sie Kommunikationsdaten für die Erstellung des Chat-Skripts.	„So erstellen Sie die Anweisungen zum Aufrufen eines Peers“ auf Seite 461

TABELLE 17–2 Übersicht der Schritte zum Einrichten des Hinauswahlrechners *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
5. Konfigurieren von Informationen zu einem bestimmten Peer	Konfigurieren Sie die PPP-Optionen zum Aufrufen eines bestimmten Einwahlservers.	„So definieren Sie die Verbindung mit einem bestimmten Peer“ auf Seite 462
6. Aufrufen des Peers	Geben Sie den Befehl `pppd` ein, um die Kommunikation zu initiieren.	„So rufen Sie den Einwahlserver auf“ auf Seite 469

Vorlagendateien für PPP-Einwahlverbindungen

Solaris PPP 4.0 bietet Vorlagendateien. Jede Vorlage enthält allgemeine Optionen für eine bestimmte PPP-Konfigurationsdatei. In der folgenden Tabelle sind die Beispielvorlagen aufgelistet, die verwendet werden können, um eine Einwahlverbindung und die entsprechenden Solaris PPP 4.0-Dateien einzurichten.

Vorlagendatei	PPP-Konfigurationsdatei	Siehe
`/etc/ppp/options.tmpl`	`/etc/ppp/options`	„`/etc/ppp/options.tmpl`-Vorlage“ auf Seite 530
`/etc/ppp/options.ttya.tmpl`	`/etc/ppp/options.`*ttyname*	„`options.ttya.tmpl`-Vorlagendatei“ auf Seite 533
`/etc/ppp/myisp-chat.tmpl`	Datei mit einem von Ihnen gewählten beliebigen Namen, die das Chat-Skript enthält	„`/etc/ppp/myisp-chat.tmpl`-Chat-Skript-Vorlage“ auf Seite 541
`/etc/ppp/peers/myisp.tmpl`	`/etc/ppp/peers/`*peer-name*	„`/etc/ppp/peers/myisp.tmpl`-Vorlagendatei“ auf Seite 536

Wenn Sie eine der Vorlagendateien verwenden, müssen Sie die betreffende Vorlage umbenennen, damit sie mit dem Namen der entsprechenden PPP-Konfigurationsdatei übereinstimmt. Die einzige Ausnahme ist die Chat-Datei-Vorlage `/etc/ppp/myisp-chat.tmpl`. Für Ihr Chat-Skript können Sie einen beliebigen Namen auswählen.

Konfigurieren von Geräten des Hinauswahlrechners

Der erste Schritt zum Einrichten eines PPP-Hinauswahlrechners besteht darin, die Geräte der seriellen Verbindung zu konfigurieren: das Modem und den seriellen Port.

Hinweis – Die Aufgaben zum Einrichten eines Modems gelten allgemein auch für eine ISDN TA-Konfiguration.

Bevor Sie zum nächsten Verfahren übergehen, führen Sie Folgendes aus:

- Installieren Sie Solaris auf dem Hinauswahlrechner.
- Legen Sie die optimale Modemgeschwindigkeit fest.
- Legen Sie fest, welcher serielle Port des Hinauswahlrechners verwendet werden soll.
- Stellen Sie das Root-Passwort für den Hinauswahlrechner bereit.

Informationen zur Planung finden Sie in Tabelle 16–2.

▼ So konfigurieren Sie das Modem und den seriellen Port (Hinauswahlrechner)

1 **Programmieren Sie das Modem.**

Zwar gibt es eine Reihe von Modemtypen, aber die meisten Modems werden mit den richtigen Einstellungen für Solaris PPP 4.0 geliefert. Die folgende Liste enthält die grundlegenden Parametereinstellungen für Modems, die Solaris PPP 4.0 verwenden.

- **DCD –** Folgen Sie den Anweisungen des Netzbetreibers.
- **DTR –** Setzen Sie diese Einstellung auf einen niedrigen Wert, sodass das Modem "auflegt" und frei wird.
- **Flusskontrolle –** Setzen Sie diese Option auf RTS/CTS für die Vollduplex-Hardware-Flusskontrolle.
- **Abrufsequenzen –** Deaktivieren

Wenn Sie Probleme beim Einrichten der Verbindung haben und vermuten, dass das Modem einen Fehler hat, ziehen Sie zunächst die Dokumentation des Modemherstellers heran. Auch bieten einige Websites Hilfe bei der Modemprogrammierung. Außerdem finden Sie Hinweise für die Behebung von Modemproblemen unter „So diagnostizieren Sie Modemprobleme“ auf Seite 515.

2 **Schließen Sie die Modemkabel an den seriellen Port des Hinauswahlrechners und die Telefonbuchse an.**

3. **Melden Sie sich als Superuser beim Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

4. **Führen Sie den Befehl `/usr/sadm/bin/smc` aus. Informationen zur Vorgehensweise finden Sie unter „Setting Up Terminals and Modems With Serial Ports Tool (Overview)“ in *System Administration Guide: Advanced Administration* . Dieser Befehl dient zum Öffnen der Solaris Management Console.**

   Verwenden Sie die Solaris Management Console für folgende Zwecke:

   a. **Wählen Sie den Port aus, an den das Modem angeschlossen ist.**

   b. **Legen Sie für die Modemrichtung die Option "nur Hinauswahl" fest.**

      Sie können das Modem als bidirektrionales Modem einrichten. Die Option "nur Hinauswahl" bietet jedoch mehr Schutz vor Eindringlingen.

Hinweis – Die Baudrate und die Zeitüberschreitung können Sie über `/usr/sadm/bin/smc` festlegen. Der `pppd`-Dämon ignoriert diese Einstellungen jedoch.

---

5. **Klicken Sie auf "OK", um die Änderungen zu übernehmen.**

Konfigurieren der Kommunikation des Hinauswahlrechners

Die in diesem Abschnitt beschriebenen Verfahren zeigen, wie die Kommunikation über die serielle Verbindung des Hinauswahlrechners konfiguriert wird. Bevor Sie diese Verfahren verwenden können, müssen Sie das Modem und den seriellen Port konfigurieren. Informationen zur Vorgehensweise finden Sie unter „So konfigurieren Sie das Modem und den seriellen Port (Hinauswahlrechner)“ auf Seite 458.

Die nächsten Aufgaben zeigen, wie der Hinauswahlrechner aktiviert wird, um die Kommunikation mit dem Einwahlserver zu initiieren. Die Kommunikation wird entsprechend den Optionen initiiert, die in den PPP-Konfigurationsdateien definiert sind. Die folgenden Dateien müssen erstellt werden:

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*
- Chat-Skript
- `/etc/ppp/peers/`*peer-name*

In Solaris PPP 4.0 sind Vorlagen für die PPP-Konfigurationsdateien enthalten, die Sie anpassen können, um Ihre Anforderungen zu erfüllen. Ausführliche Informationen zu diesen Dateien finden Sie unter „Vorlagendateien für PPP-Einwahlverbindungen“ auf Seite 457.

▼ So definieren Sie die Kommunikation über die serielle Verbindung

1 **Melden Sie sich als Superuser beim Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Erstellen Sie eine Datei namens `/etc/ppp/options` mit dem folgenden Eintrag:**

```
lock
```

Die Datei `/etc/ppp/options` wird zum Definieren der globalen Parameter verwendet, die für die gesamte Kommunikation des lokalen Rechners gelten. Die Option `lock` dient zum UUCP-basierten Sperren des Formulars `/var/spool/locks/LK.xxx.yyy.zzz` .

Hinweis – Wenn der Hinauswahlrechner keine `/etc/ppp/options`-Datei hat, kann nur der Superuser den `pppd`-Befehl ausführen. Die Datei `/etc/ppp/options` kann jedoch leer sein.

Eine vollständige Beschreibung von `/etc/ppp/options` finden Sie unter „`/etc/ppp/options`-Konfigurationsdatei“ auf Seite 530.

3 **(Optional) Erstellen Sie eine Datei namens `/etc/ppp/options.`*ttyname*, um zu definieren, wie die Kommunikation über einen bestimmten seriellen Port initiiert werden kann.**

Das nächste Beispiel zeigt eine `/etc/ppp/options.` *ttyname*-Datei für den Port mit dem Gerätenamen `/dev/cua/a` .

```
# cat /etc/ppp/options.cua.a
crtscts
```

Über die PPP-Option `crtscts` wird dem `pppd`-Dämon mitgeteilt, die Hardware-Flusskontrolle für den seriellen Port a zu aktivieren.

Weitere Informationen zur Datei `/etc/ppp/options.ttyname` finden Sie unter „`/etc/ppp/options.` *ttyname*-Konfigurationsdatei“ auf Seite 531.

4 **Stellen Sie die Modemgeschwindigkeit ein. Informationen zur Vorgehensweise finden Sie unter „So legen Sie die Modemgeschwindigkeit fest“ auf Seite 465.**

So erstellen Sie die Anweisungen zum Aufrufen eines Peers

Bevor der Hinauswahlrechner eine PPP-Verbindung initiieren kann, müssen Sie Informationen über den Einwahlserver sammeln, der als Peer verwendet werden soll. Anschließend verwenden Sie diese Informationen, um ein Chat-Skript zu erstellen, in dem die Kommunikation zwischen Hinauswahlrechner und Peer beschrieben ist.

1. **Legen Sie die Geschwindigkeit für den Hinauswahlrechner des Modems fest.**

   Weitere Informationen finden Sie unter „Konfigurieren der Modemgeschwindigkeit für eine Wählverbindung“ auf Seite 538.

2. **Rufen Sie folgende Informationen von der Site des Einwahlservers ab:**

   - Telefonnummer des Servers
   - Das verwendete Authentifizierungsprotokoll (sofern benötigt)
   - Die Anmeldesequenz, die vom Peer für das Chat-Skript benötigt wird

3. **Rufen Sie die Namen und IP-Adressen der Namenserver von der Site des Einwahlservers ab.**

4. **Stellen Sie in einem Chat-Skript Anweisungen zum Initiieren von Aufrufen an den betreffenden Peer bereit.**

   Sie können beispielsweise das folgende Chat-Skript, `/etc/ppp/mychat` , erstellen, um den Einwahlserver `myserver` aufzurufen:

```
SAY "Calling the peer\n"
        TIMEOUT 10
        ABORT BUSY
        ABORT 'NO CARRIER'
        ABORT ERROR
        REPORT CONNECT
        "" AT&F1&M5S2=255
        TIMEOUT 60
        OK ATDT1-123-555-1234
        CONNECT \c
        SAY "Connected; logging in.\n"
        TIMEOUT 5
        ogin:--ogin: pppuser
        TIMEOUT 20
        ABORT 'ogin incorrect'
        ssword: \qmypassword
        "% " \c
        SAY "Logged in.  Starting PPP on peer system.\n"
        ABORT 'not found'
        "" "exec pppd"
        ~ \c
```

   Das Skript enthält Anweisungen zum Aufrufen eines Einwahlservers von Solaris, der eine Anmeldesequenz benötigt. Eine Beschreibung der einzelnen Anweisungen finden Sie unter „Grundlegendes Chat-Skript, das für eine UNIX-basierte Anmeldung erweitert wurde“

auf Seite 543. Ausführliche Informationen zum Erstellen eines Chat-Skripts finden Sie im Abschnitt „Definieren der Kommunikation über die Einwahlverbindung“ auf Seite 538.

Hinweis – Sie rufen das Chat-Skript nicht direkt auf. Stattdessen verwenden Sie den Dateinamen des Chat-Skripts als Argument für den Befehl `chat`, durch den das Skript dann aufgerufen wird.

Wenn Solaris oder ein ähnliches Betriebssystem von einem Peer ausgeführt wird, können Sie das zuvor verwendete Chat-Skript als Vorlage für Ihre Hinauswahlrechner verwenden.

▼ So definieren Sie die Verbindung mit einem bestimmten Peer

1 **Melden Sie sich als Superuser beim Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Aktualisieren Sie die DNS-Datenbank, indem Sie die folgende `/etc/resolv.conf`-Datei erstellen:**

```
domain bigcompany.com
nameserver 10.10.111.15
nameserver 10.10.130.8
```

`domain bigcompany.com`
Gibt an, dass die DNS-Domain des Peers `bigcompany.com` ist.

`nameserver 10.10.111.15` und **`nameserver 10.10.130.8`**
Listet die IP-Adressen des Namenservers von `bigcompany.com` auf.

3 **Bearbeiten Sie die Datei `/etc/nsswitch.conf`, damit die DNS-Datenbank zuerst nach Hostinformationen durchsucht wird.**

```
hosts:      dns [NOTFOUND=return] files
```

4 **Erstellen Sie eine Datei für den Peer.**

Sie können beispielsweise die folgende Datei erstellen, um den Einwahlserver `myserver` zu definieren:

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
noauth
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
```

/dev/cua/a
: Gibt an, dass das Gerät `/dev/cua/a` als serielle Schnittstelle für Aufrufe an `myserver` verwendet werden soll.

57600
: Definiert die Geschwindigkeit der Verbindung.

noipdefault
: Gibt an, dass der Hinauswahlrechner für Transaktionen mit dem Peer `myserver` anfangs die IP-Adresse 0.0.0.0. hat. `myserver` weist dem Hinauswahlrechner für jede Wählsitzung eine IP-Adresse zu.

idle 120
: Gibt für die Verbindung ein Zeitlimit von 120 Sekunden an.

noauth
: Gibt an, dass der Peer `myserver` keine Authentifizierungs-Berechtigungsnachweise bereitstellen muss, wenn die Verbindung mit dem Hinauswahlrechner ausgehandelt wird.

connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
: Gibt die Option `connect` und ihre Argumente an, einschließlich der Telefonnummer des Peers und des Chat-Skripts `/etc/ppp/mychat` mit den Aufrufanweisungen.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- Informationen zum Konfigurieren eines weiteren Hinauswahlrechners finden Sie unter „So konfigurieren Sie das Modem und den seriellen Port (Hinauswahlrechner)“ auf Seite 458.
- Informationen zum Testen der Modemkonnektivität mittels Anwahl eines anderen Computers finden Sie auf den Manpages `cu(1C)` und `tip(1)`. Mit diesen Dienstprogrammen können Sie prüfen, ob Ihr Modem richtig konfiguriert ist. Diese Dienstprogramme können Sie auch dazu verwenden, um eine Verbindung mit einem anderen Rechner herzustellen.
- Weitere Informationen zu den Konfigurationsdateien und Optionen finden Sie unter „Verwenden von PPP-Optionen in Dateien und in der Befehlszeile“ auf Seite 525.
- Informationen zum Konfigurieren eines Einwahlservers finden Sie unter „Konfigurieren von Geräten auf dem Einwahlserver“ auf Seite 464.

Konfigurieren des Einwahlservers

Die in diesem Abschnitt beschriebenen Aufgaben dienen zum Konfigurieren des Einwahlservers. Der Einwahlserver ist ein Peer-Rechner, der Aufrufe des Hinauswahlrechners über eine PPP-Verbindung empfängt. Die Aufgaben zeigen, wie der Einwahlserver `myserver` konfiguriert wird, der in Abbildung 16–1 dargestellt wird.

Aufgaben zum Konfigurieren des Einwahlservers (Übersicht der Schritte)

TABELLE 17–3 Übersicht der Schritte zum Einrichten des Einwahlservers

Aufgabe	Beschreibung	Siehe
1. Sammeln von Informationen vor der Konfiguration	Sammeln Sie vor dem Einrichten der Verbindung die benötigten Daten, beispielsweise Peer-Hostnamen, Zieltelefonnummern und Modemgeschwindigkeit.	„Planen einer PPP-Einwahlverbindung“ auf Seite 438
2. Konfigurieren des Modems und des seriellen Ports	Richten Sie das Modem und den seriellen Port ein.	„So konfigurieren Sie das Modem und den seriellen Port (Einwahlserver)“ auf Seite 464
3. Konfigurieren des Abrufs von Peer-Informationen	Richten Sie die Benutzerumgebungen und PPP-Optionen für jeden Hinauswahlrechner ein, dem erlaubt ist, den Einwahlserver aufzurufen.	„So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466
4. Konfigurieren der Kommunikation über eine serielle Verbindung	Konfigurieren Sie die Eigenschaften der Kommunikation über eine serielle Verbindung.	„So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)“ auf Seite 468

Konfigurieren von Geräten auf dem Einwahlserver

Im folgenden Verfahren wird beschrieben, wie das Modem und der serielle Port auf dem Einwahlserver konfiguriert werden.

Bevor Sie mit dem nächsten Verfahren fortfahren, führen Sie folgende Schritte aus, um den Peer-Einwahlserver zu konfigurieren:

- Installieren Sie Solaris.
- Legen Sie die optimale Modemgeschwindigkeit fest.
- Legen Sie fest, welcher serielle Port verwendet werden soll.

▼ So konfigurieren Sie das Modem und den seriellen Port (Einwahlserver)

1 **Programmieren Sie das Modem entsprechend den Anweisungen in der Dokumentation des Modemherstellers.**

Weitere Informationen und Hinweise finden Sie unter „So konfigurieren Sie das Modem und den seriellen Port (Hinauswahlrechner)“ auf Seite 458.

2. **Schließen Sie das Modem an den seriellen Port des Einwahlservers an.**

3. **Melden Sie sich als Superuser beim Einwahlserver oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

4. **Konfigurieren Sie den seriellen Port mithilfe des Befehls `/usr/sadm/bin/smc` für die Solaris Management Console. Informationen zur Vorgehensweise finden Sie unter „Setting Up Terminals and Modems With Serial Ports Tool (Overview)“ in *System Administration Guide: Advanced Administration* .**

   Verwenden Sie die Solaris Management Console, um wie folgt vorzugehen:

   a. **Wählen Sie den seriellen Port aus, an den das Modem angeschlossen ist.**

   b. **Legen Sie für die Modemrichtung "nur Einwahl" fest.**

      Hinweis – Solaris PPP 4.0 unterstützt die bidirektionale Kommunikation für ein Modem.

   c. **Klicken Sie auf "OK", um die Änderungen zu übernehmen.**

▼ So legen Sie die Modemgeschwindigkeit fest

Im folgenden Verfahren wird beschrieben, wie die Modemgeschwindigkeit für einen Einwahlserver festgelegt wird. Informationen zu Geschwindigkeiten für Sun Microsystems-Computer finden Sie unter „Konfigurieren der Modemgeschwindigkeit für eine Wählverbindung“ auf Seite 538.

1. **Melden Sie sich beim Einwahlserver an.**

2. **Verwenden Sie den Befehl `tip`, um mit dem Modem zu kommunizieren.**

   Anweisungen zur Verwendung des Befehls `tip` für die Festlegung der Modemgeschwindigkeit finden Sie auf der Manpage `tip`(1).

3. **Konfigurieren Sie das Modem für eine feste DTE-Geschwindigkeit.**

4. **Legen Sie die Geschwindigkeit für den seriellen Port fest, indem Sie `ttymon` oder `/usr/sadm/bin/smc` verwenden. Informationen zur Vorgehensweise finden Sie unter „Setting Up Terminals and Modems With Serial Ports Tool (Overview)“ in *System Administration Guide: Advanced Administration* .**

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „So konfigurieren Sie das Modem und den seriellen Port (Einwahlserver)“ auf Seite 464
- „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466

Einrichten von Benutzern der Einwahlservers

Ein Teil des Verfahrens zum Einrichten eines Einwahlservers besteht darin, Informationen zu konfigurieren, die jeden bekannten Remote-Anrufer betreffen.

Bevor Sie mit den in diesem Abschnitt beschriebenen Verfahren beginnen, führen Sie Folgendes aus:

- Stellen Sie die UNIX-Benutzernamen für alle Benutzer bereit, denen erlaubt ist, sich über Remote-Hinauswahlrechner anzumelden.
- Richten Sie das Modem und eine serielle Verbindung ein. Informationen zur Vorgehensweise finden Sie unter „So konfigurieren Sie das Modem und den seriellen Port (Einwahlserver)“ auf Seite 464.
- Weisen Sie den eingehenden Aufrufen von Remote-Benutzern eine dedizierte IP-Adresse zu. Eine dedizierte IP-Adresse für eingehende Aufrufe kann erstellt werden, wenn die Anzahl der potenziellen Anrufer größer ist als die Anzahl der Modems und seriellen Ports auf dem Einwahlserver. Vollständige Informationen zum Erstellen dedizierter IP-Adressen finden Sie unter „Erstellen eines IP-Adressierungsschemas für Anrufer“ auf Seite 556.

▼ So konfigurieren Sie Benutzer des Einwahlservers

1 Melden Sie sich als Superuser beim Einwahlserver oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Erstellen Sie für jeden Remote-PPP-Benutzer ein neues Konto auf dem Einwahlserver.

Zum Erstellen eines neuen Benutzers können Sie die Solaris Management Console verwenden. Der Befehl `/usr/sadm/bin/smc` dient zum Öffnen der Solaris Management Console. Anweisungen zum Erstellen eines neuen Benutzers mithilfe der Solaris Management Console finden Sie unter „Setting Up User Accounts (Task Map)“ in *System Administration Guide: Basic Administration* .

3 Verwenden Sie die Solaris Management Console, um Parameter für den neuen Benutzer zuzuweisen.

Die folgende Tabelle enthält die Parameter für ein Konto namens `pppuser` für `user1` auf dem Hinauswahlrechner `myhome`.

Parameter	Wert	Definition
Benutzername	`pppuser`	Der Name des Benutzerkontos für den Remote-Benutzer. Dieser Kontoname sollte mit dem Kontonamen übereinstimmen, der in der Anmeldesequenz des Chat-Skripts angegeben ist. `pppuser` ist beispielsweise der Kontoname, der im Chat-Skript enthalten ist, das unter „So erstellen Sie die Anweisungen zum Aufrufen eines Peers“ auf Seite 461 beschrieben wird.
Anmelde-Shell	`/usr/bin/pppd`	Die standardmäßige Anmelde-Shell für den Remote-Benutzer. Die Anmelde-Shell `/usr/bin/pppd` beschränkt den Anrufer anfangs auf eine dedizierte PPP-Umgebung.
Erstellung des Home-Verzeichnispfads	`/export/home/pppuser`	Das Home-Verzeichnis `/export/home/pppuser` wird festgelegt, wenn sich ein Anrufer erfolgreich beim Einwahlserver angemeldet hat.

4 Erstellen Sie für jeden Anrufer eine `$HOME/.pprc`-Datei, in der verschiedene spezifische Optionen für die PPP-Sitzung des Benutzers enthalten sind.

Sie können beispielsweise die folgende `.ppprc`-Datei für `pppuser` erstellen.

```
# cat /export/home/pppuser/.ppprc
noccp
```

`noccp` deaktiviert die Komprimierungssteuerung der Verbindung.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466.
- „So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)“ auf Seite 468.

Konfigurieren der Kommunikation über den Einwahlserver

Die nächste Aufgabe zeigt, wie der Einwahlserver aktiviert wird, um die Kommunikation mit einem Hinauswahlrechner herzustellen. Die Kommunikation wird entsprechend den Optionen hergestellt, die in den folgenden PPP-Konfigurationsdateien definiert sind:

- `/etc/ppp/options`
- `/etc/ppp/options.`*`ttyname`*

Ausführliche Informationen zu diesen Dateien finden Sie unter „Verwenden von PPP-Optionen in Dateien und in der Befehlszeile“ auf Seite 525.

Bevor Sie fortfahren, führen Sie folgende Schritte aus:

- Konfigurieren Sie den seriellen Port und das Modem auf dem Einwahlserver. Informationen zur Vorgehensweise finden Sie unter „So konfigurieren Sie das Modem und den seriellen Port (Einwahlserver)“ auf Seite 464.
- Konfigurieren Sie Informationen zu den potenziellen Benutzern des Einwahlservers. Informationen zur Vorgehensweise finden Sie unter „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466.

▼ So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)

1 Melden Sie sich als Superuser beim Einwahlserver oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Erstellen Sie die `/etc/ppp/options`-Datei mithilfe des folgenden Eintrags:

```
nodefaultroute
```

`nodefaultroute` zeigt an, dass keine `pppd`-Sitzung auf dem lokalen Rechner eine Standardroute ohne `root`-Berechtigungen herstellen kann.

Hinweis – Wenn der Einwahlserver keine `/etc/ppp/options`-Datei hat, kann nur der Superuser den `pppd`-Befehl ausführen. Die `/etc/ppp/options`-Datei kann jedoch leer sein.

---

3 Erstellen Sie die Datei `/etc/options.` *ttyname*, um zu definieren, wie Anrufe, die über den seriellen Port *ttyname* eingehen, gehandhabt werden sollen.

Die folgende `/etc/options.ttya`-Datei definiert, wie der serielle Port `/dev/ttya` des Einwahlservers eingehende Anrufe handhaben soll:

```
:10.0.0.80
xonxoff
```

`:10.0.0.80`	Weist die IP-Adresse 10.0.0.80 allen Peers zu, die sich über den seriellen Port `ttya` einwählen.
`xonxoff`	Erlaubt der seriellen Verbindung, die Kommunikation von Modems mit aktivierter Software-Flusskontrolle zu steuern.

Siehe auch Wenn Sie alle in diesem Kapitel aufgeführten Verfahren durchgeführt haben, ist die Konfiguration der Einwahlverbindung abgeschlossen. Die folgende Liste enthält Verweise auf relevante Informationen:

- Informationen zum Testen der Modemkonnektivität mittels Anwahl eines anderen Computers finden Sie auf den Manpages `cu(1C)` und `tip(1)`. Mit diesen Dienstprogrammen können Sie prüfen, ob Ihr Modem richtig konfiguriert ist. Diese Dienstprogramme können Sie auch dazu verwenden, um eine Verbindung mit einem anderen Rechner herzustellen.
- Informationen zum Konfigurieren weiterer Optionen für den Einwahlserver finden Sie unter „Konfigurieren des Einwahlservers“ auf Seite 463.
- Informationen zum Konfigurieren weiterer Hinauswahlrechner finden Sie unter „Konfigurieren des Hinauswahlrechners“ auf Seite 456.
- Informationen darüber, wie Sie den Einwahlserver vom Remote-Rechner aufrufen lassen, finden Sie unter „Aufrufen des Einwahlservers“ auf Seite 469.

Aufrufen des Einwahlservers

Richten Sie eine PPP-Wählverbindung ein, indem Sie den Einwahlserver vom Hinauswahlrechner aufrufen lassen. Sie können den Hinauswahlrechner anweisen, den Server aufzurufen, indem Sie die Option `demand` in den lokalen PPP-Konfigurationsdateien angeben. Die gebräuchlichste Methode zum Herstellen der Verbindung besteht jedoch darin, dass der Benutzer den Befehl `pppd` auf dem Hinauswahlrechner ausführt.

Bevor Sie mit der nächsten Aufgabe fortfahren, sollten Sie eine oder beide der folgenden Aufgaben ausgeführt haben:

- Richten Sie den Hinauswahlrechner ein. Informationen hierzu finden Sie unter „Konfigurieren des Hinauswahlrechners“ auf Seite 456.
- Richten Sie den Einwahlserver ein. Informationen hierzu finden Sie unter „Konfigurieren des Einwahlservers“ auf Seite 463.

▼ So rufen Sie den Einwahlserver auf

1. **Melden Sie sich beim Hinauswahlrechner an, indem Sie Ihr normales Benutzerkonto verwenden. Melden Sie sich jedoch nicht als Root-Benutzer an.**

2. **Rufen Sie den Einwahlserver auf, indem Sie den Befehl `pppd` ausführen.**

   Beispielsweise initiiert der folgende Befehl eine Verbindung zwischen dem Hinauswahlrechner und dem Einwahlserver `myserver`:

   ```
   % pppd 57600 call myserver
   ```

pppd	Startet den Aufruf durch Aufrufen des pppd-Dämons.
57600	Legt die Geschwindigkeit der Verbindung zwischen Host und Modem fest.
call myserver	Ruft die call-Option von pppd auf. pppd liest dann die Optionen in der Datei /etc/ppp/peers/myserver, die in dem Verfahren erstellt wurde, das unter „So definieren Sie die Verbindung mit einem bestimmten Peer“ auf Seite 462 beschrieben ist.

3 Stellen Sie Kontakt mit einem Host im Netzwerk des Servers her, beispielsweise mit dem Host lindyhop, der in Abbildung 16–1 dargestellt ist:

```
ping lindyhop
```

Wenn die Verbindung nicht richtig funktioniert, lesen Sie Kapitel 21, „Beheben von allgemeinen PPP-Problemen (Aufgaben)“.

4 Beenden Sie die PPP-Sitzung:

```
% pkill -x pppd
```

Siehe auch Wenn Sie alle in diesem Kapitel aufgeführten Verfahren durchgeführt haben, ist die Konfiguration der Wählverbindung abgeschlossen. Die folgende Liste enthält Verweise auf relevante Informationen:

- Informationen darüber, was zu tun ist, damit die Benutzer ihre Hinauswahlrechner verwenden können, finden Sie unter „So rufen Sie den Einwahlserver auf“ auf Seite 469.
- Um Verbindungsprobleme zu beheben, lesen Sie Kapitel 21, „Beheben von allgemeinen PPP-Problemen (Aufgaben)“.
- Weitere Informationen zu den Dateien und Optionen, die in diesem Kapitel verwendet werden, finden Sie unter „Verwenden von PPP-Optionen in Dateien und in der Befehlszeile“ auf Seite 525.

◆ ◆ ◆ KAPITEL 18

Einrichten einer PPP-Standleitungsverbindung (Aufgaben)

In diesem Kapitel wird beschrieben, wie eine PPP-Verbindung konfiguriert wird, für die eine Standleitung zwischen Peers verwendet wird. In den Hauptabschnitten werden folgende Themen behandelt:

- „Konfigurieren von synchronen Geräten an der Standleitung“ auf Seite 472
- „Konfigurieren eines Rechners an der Standleitung“ auf Seite 473

Einrichten einer Standleitung (Übersicht der Schritte)

Standleitungsverbindungen können im Vergleich mit Wählverbindungen relativ unkompliziert eingerichtet werden. In den meisten Fällen müssen Sie keine CSUs/DSUs, Wählservices oder Authentifizierungen konfigurieren. Wenn Sie ein CSU/DSU konfigurieren müssen, sollten Sie die Herstellerdokumentation heranziehen, da dies eine komplizierte Aufgabe ist.

Die Übersicht der Schritte in der folgenden Tabelle zeigt alle Aufgaben, die mit dem Einrichten der grundlegenden Standleitungsverbindung verbunden sind.

Hinweis – Manche Standleitungen erfordern ein CSU/DSU, um die Adresse des Peers am anderen Ende der Leitung anzuwählen. Beispielsweise verwendet Frame Relay den SVCs-Service (Switched Virtual Circuits) oder Switched 56-Service.

TABELLE 18–1 Übersicht der Schritte zum Einrichten der Standleitungsverbindung

Aufgabe	Beschreibung	Siehe
1. Sammeln von Informationen vor der Konfiguration	Sammeln Sie vor dem Einrichten der Verbindung die benötigten Daten.	Tabelle 16–4

TABELLE 18–1 Übersicht der Schritte zum Einrichten der Standleitungsverbindung *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
2. Einrichten der Standleitungshardware	Installieren Sie das CSU/DSU und die synchrone Schnittstellenkarte.	„So konfigurieren Sie synchrone Geräte“ auf Seite 472
3. Konfigurieren der Schnittstellenkarte (bei Bedarf)	Konfigurieren Sie das Schnittstellenskript, das verwendet werden soll, wenn die Standleitung initiiert wird.	„So konfigurieren Sie synchrone Geräte“ auf Seite 472
4. Konfigurieren von Informationen zum Remote-Peer	Definieren Sie, wie die Kommunikation zwischen Ihrem lokalen Rechner und dem Remote-Peer ablaufen soll.	„So konfigurieren Sie einen Rechner an einer Standleitung“ auf Seite 474
5. Starten der Standleitung	Konfigurieren Sie Ihren Rechner so, dass PPP als Teil des Boot-Vorgangs über die Standleitung gestartet wird.	„So konfigurieren Sie einen Rechner an einer Standleitung“ auf Seite 474

Konfigurieren von synchronen Geräten an der Standleitung

In der nächsten Aufgabe wird beschrieben, wie Geräte für die Standleitungstopologie konfiguriert werden (siehe „Beispielkonfiguration für eine Standleitungsverbindung“ auf Seite 443). Zu den synchronen Geräten, die für die Standleitung benötigt werden, gehören eine Schnittstelle und ein Modem.

Voraussetzungen für das Einrichten von synchronen Geräten

Bevor Sie zum nächsten Verfahren übergehen, führen Sie folgende Schritte aus:

- Lassen Sie von Ihrem Provider ein Standleitung installieren.
- Ein synchrones Gerät (CSU/DSU)
- Solaris auf Ihrem Rechner
- Die für Ihren Rechner erforderliche synchrone Schnittstellenkarte

▼ So konfigurieren Sie synchrone Geräte

1 Installieren Sie bei Bedarf die Schnittstellenkarte physisch auf dem lokalen Rechner.

Folgen Sie den Anweisungen in der Herstellerdokumentation.

2 Verbinden Sie die Kabel des CSU/DSU mit der Schnittstelle.

Verbinden Sie bei Bedarf die Kabel des CSU/DSU mit der Buchse der Standleitung oder einem ähnlichen Anschluss.

3 **Konfigurieren Sie das CSU/DSU entsprechend den Anweisungen in der Dokumentation des Herstellers oder Netzbetreibers.**

Hinweis – Der Provider, bei dem Sie die Standleitung gemietet haben, kann möglicherweise das CSU/DSU für Ihre Verbindung konfigurieren.

---

4 **Konfigurieren Sie bei Bedarf die Schnittstellenkarte anhand der entsprechenden Dokumentation.**

Die Konfiguration der Schnittstellenkarte erfordert die Erstellung eines Startskripts für die Schnittstelle. Der Router in der in Abbildung 16–2 dargestellten Standleitungskonfiguration von LocalCorp verwendet eine HSI/P-Schnittstellenkarte.

Das folgende Skript, `hsi-conf`, startet die HSI/P-Schnittstelle.

```
#!/bin/ksh
/opt/SUNWconn/bin/hsip_init hihp1 speed=1536000 mode=fdx loopback=no \
nrzi=no txc=txc rxc=rxc txd=txd rxd=rxd signal=no 2>&1 > /dev/null
```

`hihp1`	Zeigt an, dass HSI/P der verwendete synchrone Port ist.
`speed=1536000`	Einstellung zum Anzeigen der Geschwindigkeit des CSU/DSU

Siehe auch Informationen zum Konfigurieren des lokalen Rechners an der Standleitung finden Sie unter „So konfigurieren Sie einen Rechner an einer Standleitung“ auf Seite 474.

Konfigurieren eines Rechners an der Standleitung

Die in diesem Abschnitt enthaltene Aufgabe zeigt, wie ein Router eingerichtet wird, um an Ihrem Ende der Standleitung als lokaler Peer zu fungieren. In der Aufgabe wird die Standleitung verwendet, die unter „Beispielkonfiguration für eine Standleitungsverbindung“ auf Seite 443 als Beispiel angeführt ist.

Voraussetzungen zum Konfigurieren des lokalen Rechners an einer Standleitung

Bevor Sie zum nächsten Verfahren übergehen, führen Sie die folgenden Schritte aus:

- Richten Sie die synchronen Geräte für die Verbindung ein, und konfigurieren Sie sie. Informationen zur Vorgehensweise finden Sie unter „Konfigurieren von synchronen Geräten an der Standleitung“ auf Seite 472.
- Stellen Sie das Root-Passwort für den lokalen Rechner an der Standleitung bereit.

- Richten Sie den lokalen Rechner als Netzwerkrouter ein, um die Services des Providers der Standleitung zu nutzen.

So konfigurieren Sie einen Rechner an einer Standleitung

1 Melden Sie sich als Superuser beim lokalen Rechner (Router) oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie einen Eintrag für den Remote-Peer in die `/etc/hosts`-Datei des Routers ein.

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
192.168.130.10  local2-peer        loghost
192.168.130.11  local1-net
10.0.0.25       farISP
```

Die `/etc/hosts`-Beispieldatei ist für den lokalen Router des fiktiven Unternehmens LocalCorp bestimmt. Beachten Sie die IP-Adresse und den Hostnamen für den Remote-Peer `farISP` am Standort des Serviceproviders.

3 Erstellen Sie die Datei `/etc/ppp/peers/`*peer-name*, in der die Informationen zum Peer des Providers gespeichert werden.

Für diese als Beispiel dienende Standleitungsverbindung erstellen Sie die Datei `/etc/ppp/peers/farISP`.

```
# cat /etc/ppp/peers/farISP
init '/etc/ppp/conf_hsi'
local
/dev/hihp1
sync
noauth
192.168.130.10:10.0.0.25
passive
persist
noccp
nopcomp
novj
noaccomp
```

In der folgenden Tabelle werden die Optionen und Parameter erläutert, die in `/etc/ppp/peers/farISP` verwendet werden.

Option	Definition
`init '/etc/ppp/conf_hsi'`	Startet die Verbindung. `init` konfiguriert dann die HSI-Schnittstelle mithilfe der Parameter im Skript `/etc/ppp/conf_hsi` .
`local`	Teilt dem `pppd`-Dämon mit, nicht den Status des DTR-Signals (Data Terminal Ready) zu ändern. Teilt `pppd` außerdem mit, das DCD-Eingangssignal (Data Carrier Detect) zu ignorieren.
`/dev/hihp1`	Gibt den Gerätenamen der synchronen Schnittstelle an.
`sync`	Richtet die synchrone Codierung für die Verbindung ein.
`noauth`	Legt fest, dass das lokale System keine Authentifizierung vom Peer verlangt. Der Peer kann allerdings eine Authentifizierung verlangen.
`192.168.130.10:10.0.0.25`	Definiert die IP-Adresse des lokalen Peers und des Remote-Peers. Als Trennzeichen wird ein Doppelpunkt verwendet.
`passive`	Teilt dem `pppd`-Dämon auf dem lokalen Rechner mit, nach der Ausgabe der maximalen Anzahl von LCP-Konfigurationsanforderungen passiv zu bleiben und auf den Start des Peers zu warten.
`persist`	Teilt dem `pppd`-Dämon mit, nach der Beendigung einer Verbindung zu versuchen, die Verbindung neu zu starten.
`noccp, nopcomp, novj, noaccomp`	Deaktiviert das CCP (Compression Control Protocol), die Protocol Field-Komprimierung, die Van Jacobson-Komprimierung und die Adressen- und Steuerfeldkomprimierung. Diese Formen der Komprimierung beschleunigen die Übertragung über eine Einwahlverbindung. Eine Standleitung kann dadurch allerdings verlangsamt werden.

4 Erstellt ein Initialisierungsskript namens `demand`, das die PPP-Verbindung als Teil des Boot-Vorgangs Prozesses erstellt.

```
# cat /etc/ppp/demand
#!/bin/sh
if [ -f /var/run/ppp-demand.pid ] &&
   /usr/bin/kill -s 0 ‘/bin/cat /var/run/ppp-demand.pid‘
then
        :
else
        /usr/bin/pppd call farISP
fi
```

Das `demand`-Skript enthält den Befehl `pppd`, der zum Herstellen einer Standleitungsverbindung dient. In der nachstehenden Tabellen wird der Inhalt von `$PPPDIR/demand` erläutert.

Codebeispiel	Erläuterung
`if [ -f /var/run/ppp-demand.pid ] && /usr/bin/kill -s 0 ‘/bin/cat /var/run/ppp-demand.pid‘`	Anhand dieser Zeilen wird geprüft, ob `pppd` ausgeführt wird. Wenn `pppd` ausgeführt wird, muss `pppd` nicht gestartet werden.

Codebeispiel	Erläuterung
`/usr/bin/pppd call farISP`	Mit dieser Zeile wird `pppd` gestartet. `pppd` liest die Optionen von `/etc/ppp/options`. Die Option `call farISP` in der Befehlszeile bewirkt, dass `/etc/ppp/peers/farISP` ebenfalls gelesen wird.

Das Solaris PPP 4.0-Startskript `/etc/rc2.d/S47pppd` ruft das `demand`-Skript als Teil des Boot-Vorgangs auf. Mit folgenden Zeilen in `/etc/rc2.dS47pppd` wird nach einer Datei namens `$PPPDIR/demand` gesucht.

```
if [ -f $PPPDIR/demand ]; then
            . $PPPDIR/demand
    fi
```

Wenn sie gefunden wird, wird `$PPPDIR/demand` ausgeführt. Während der Ausführung von `$PPPDIR/demand` wird die Verbindung hergestellt.

Hinweis – Um die Rechner außerhalb des lokalen Netzwerks zu erreichen, müssen die Benutzer `telnet`, `ftp`, `rsh` oder einen ähnlichen Befehl ausführen.

Siehe auch Wenn Sie alle in diesem Kapitel aufgeführten Verfahren durchgeführt haben, ist die Konfiguration der Standleitungsverbindung abgeschlossen. Die folgende Liste enthält Verweise auf relevante Informationen.

- Informationen zur Fehlerbehebung finden Sie unter „Beheben von Standleitungsproblemen“ auf Seite 523.
- Weitere Informationen zu den Dateien und Optionen, die in diesem Kapitel verwendet werden, finden Sie unter „Verwenden von PPP-Optionen in Dateien und in der Befehlszeile“ auf Seite 525.

◆ ◆ ◆ KAPITEL 19

Einrichten der PPP-Authentifizierung (Aufgaben)

Dieses Kapitel enthält Aufgaben zum Einrichten der PPP-Authentifizierung. Folgende Themen werden behandelt:

- „Konfigurieren der PAP-Authentifizierung“ auf Seite 478
- „Konfigurieren der CHAP-Authentifizierung “ auf Seite 486

Anhand der Verfahren wird aufgezeigt, wie die Authentifizierung über eine Wählverbindung durchgeführt wird, weil die Verwendung von Wählverbindungen zu diesem Zweck wahrscheinlicher als die Verwendung von Standleitungsverbindungen ist. Sie können die Authentifizierung über Standleitungen konfigurieren, wenn eine Authentifizierung aufgrund der Sicherheitsrichtlinien Ihres Unternehmens erforderlich ist. Für die Authentifizierung über eine Standleitung ziehen Sie die in diesem Kapitel beschriebenen Aufgaben als Orientierungshilfe zurate.

Wenn Sie die PPP-Authentifizierung verwenden möchten, sich aber nicht sicher sind, welches Protokoll zu verwenden ist, informieren Sie sich im Abschnitt „Warum die PPP-Authentifizierung verwendet werden sollte“ auf Seite 433. Weitere Informationen zur PPP-Authentifizierung finden Sie auf der Manpage pppd(1M) und unter „Authentifizieren von Anrufern“ auf Seite 549.

Konfigurieren der PPP-Authentifizierung (Übersicht der Schritte)

Die in diesem Abschnitt enthaltenen Übersichten der Schritte helfen Ihnen, rasch die richtigen Verfahren für die PPP-Authentifizierung zu finden.

TABELLE 19–1 Übersicht der Schritte für die allgemeine PPP-Authentifizierung

Aufgabe	Beschreibung	Siehe
Konfigurieren der PAP-Authentifizierung	Wenden Sie diese Verfahren an, um die PAP-Authentifizierung auf einem Einwahlserver und einem Hinauswahlrechner zu aktivieren.	„Einrichten der PAP-Authentifizierung (Übersicht der Schritte)“ auf Seite 478
Konfigurieren der CHAP-Authentifizierung	Wenden Sie diese Verfahren an, um die CHAP-Authentifizierung auf einem Einwahlserver und einem Hinauswahlrechner zu aktivieren.	„Einrichten der CHAP-Authentifizierung (Übersicht der Schritte)“ auf Seite 487

Konfigurieren der PAP-Authentifizierung

Die Aufgaben in diesem Abschnitt zeigen auf, wie die Authentifizierung über eine PPP-Verbindung mithilfe des PAP (Password Authentication Protocol) durchgeführt wird. Das verwendete Beispiel, das unter „Beispiele für PPP-Authentifizierungskonfigurationen“ auf Seite 446 aufgeführt wird, dient zur Veranschaulichung eines PAP-Szenarios für eine Einwahlverbindung. Verwenden Sie die Anweisungen als Basis für die Implementierung der PAP-Authentifizierung an Ihrem Standort.

Bevor Sie zu den nächsten Verfahren übergehen, führen Sie Folgendes aus:

- Richten Sie eine Wählverbindung zwischen dem Einwahlserver und den Hinauswahlrechnern ein, die zu vertrauenswürdigen aufrufenden Programmen gehören, und testen Sie diese Wählverbindung.
- Optimal für die Einwahlserver-Authentifizierung ist eine Superuser-Berechtigung für den Rechner, auf dem die Netzwerkpasswort-Datenbank verwaltet wird (beispielsweise in LDAP-, NIS- oder lokalen Dateien).
- Holen Sie eine Superuser-Berechtigung für den lokalen Rechner ein (entweder ein Einwahlserver oder ein Hinauswahlrechner).

Einrichten der PAP-Authentifizierung (Übersicht der Schritte)

Verwenden Sie die nächste Übersicht der Schritte, um rasch auf PAP-bezogene Aufgaben für den Einwahlserver und vertrauenswürdige aufrufende Programme auf Hinauswahlrechnern zuzugreifen.

TABELLE 19–2 Übersicht der Schritte für die PAP-Authentifizierung (Einwahlserver)

Aufgabe	Beschreibung	Siehe
1. Sammeln von Informationen vor der Konfiguration	Sammeln Sie Benutzernamen und andere Daten, die für die Authentifizierung benötigt werden.	„Planen der Authentifizierung zur Verwendung einer Verbindung“ auf Seite 445
2. Aktivieren der Passwortdatenbank (bei Bedarf)	Stellen Sie sicher, dass potenzielle aufrufende Programme in der Passwortdatenbank des Servers enthalten sind.	„So erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 480
3. Erstellen der PAP-Datenbank	Erstellen Sie Sicherheitsberechtigungsnachweise für alle potenziellen aufrufenden Programme in `/etc/ppp/pap-secrets`.	„So erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 480
4. Modifizieren der PPP-Konfigurationsdateien	Fügen Sie PAP-spezifische Optionen in die Dateien `/etc/ppp/options` und `/etc/ppp/peers/`*peer-name* ein.	„So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)“ auf Seite 481

TABELLE 19–3 Übersicht der Schritte für die PAP-Authentifizierung (Hinauswahlrechner)

Aufgabe	Beschreibung	Siehe
1. Sammeln von Informationen vor der Konfiguration	Sammeln Sie Benutzernamen und andere Daten, die für die Authentifizierung benötigt werden.	„Planen der Authentifizierung zur Verwendung einer Verbindung“ auf Seite 445
2. Erstellen der PAP-Datenbank für den Rechner des vertrauenswürdigen aufrufenden Programms	Erstellen Sie die Sicherheitsberechtigungsnachweise für das vertrauenswürdige aufrufende Programm und bei Bedarf die Sicherheitsberechtigungsnachweise für andere Benutzer, die den Hinauswahlrechner in `/etc/ppp/pap-secrets` aufrufen.	„So konfigurieren Sie PAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer“ auf Seite 483
3. Modifizieren der PPP-Konfigurationsdateien	Fügen Sie PAP-spezifische Optionen in die Dateien `/etc/ppp/options` und `/etc/ppp/peers/`*peer-name* ein.	„So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)“ auf Seite 485

Konfigurieren der PAP-Authentifizierung auf dem Einwahlserver

Zum Einrichten der PAP-Authentifizierung gehen Sie wie folgt vor:

- Erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise.
- Modifizieren Sie die PPP-Konfigurationsdateien für die PAP-Unterstützung.

▼ So erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise (Einwahlserver)

Dieses Verfahren dient zum Modifizieren der `/etc/ppp/pap-secrets`-Datei, in der die PAP-Sicherheitsberechtigungsnachweise enthalten sind, die verwendet werden, um aufrufende Programme zu authentifizieren. `/etc/ppp/pap-secrets` muss auf beiden Rechnern vorhanden sein, die über eine PPP-Verbindung kommunuzieren.

In der in Abbildung 16–3 dargestellten PAP-Beispielkonfiguration wird die `login`-Option von PAP verwendet. Wenn Sie vorhaben, diese Option zu verwenden, müssen Sie möglicherweise auch die Passwortdatenbank Ihres Netzwerks aktualisieren. Weitere Informationen zur `login`-Option finden Sie unter „Verwenden der `login`-Option mit `/etc/ppp/pap-secrets`“ auf Seite 552.

1 **Stellen Sie eine Liste aller potenziellen vertrauenswürdigen aufrufenden Programme zusammen. Vertrauenswürdige aufrufende Programme/Anrufer sind Personen, denen die Berechtigung erteilt wird, über ihre Remote-Rechner den Einwahlserver aufzurufen.**

2 **Stellen Sie sicher, dass für jedes vertrauenswürdige aufrufende Programm bereits ein UNIX-Benutzername und ein Passwort in der Passwortdatenbank des Einwahlservers enthalten sind.**

Hinweis – Diese Verifizierung ist vor allem für die PAP-Beispielkonfiguration wichtig. In dieser Konfiguration wird die `login`-Option von PAP verwendet, um Anrufer (bzw. aufrufende Programme) zu authentifizieren. Wenn Sie `login` nicht für PAP implementieren, müssen die PAP-Benutzernamen der Anrufer nicht mit den UNIX-Benutzernamen übereinstimmen. Weitere Informationen zu standardmäßigen `/etc/ppp/pap-secrets` finden Sie unter „`/etc/ppp/pap-secrets`-Datei“ auf Seite 549.

Gehen Sie wie folgt vor, wenn ein potenzieller vertrauenswürdiger Anrufer (bzw. ein aufrufdendesProgramm) weder einen UNIX-Benutzernamen noch ein Passwort hat:

a. **Lassen Sie sich von den Vorgesetzen der Anrufer, die Sie nicht persönlich kennen, bestätigen, dass diese Anrufer die Berechtigung haben, auf den Einwahlserver zuzugreifen.**

b. **Erstellen Sie UNIX-Benutzernamen und Passwörter für diese Anrufer, wobei Sie die Sicherheitsrichtlinien Ihres Unternehmens befolgen.**

3 **Melden Sie sich als Superuser beim Einwahlserver oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

4 Bearbeiten Sie die `/etc/ppp/pap-secrets` -Datei.

Diese Version bietet eine `pap-secrets`-Datei in `/etc/ppp`, die Kommentare zur Verwendung der PAP-Authentifizierung enthält, aber keine Optionen. Am Ende der Kommentare können Sie folgende Optionen eintragen:

```
user1      myserver        ""          *
user2      myserver        ""          *
myserver   user2           serverpass  *
```

Um die `login`-Option von `/etc/ppp/pap-secrets` zu verwenden, müssen Sie den UNIX-Benutzernamen jedes vertrauenswürdigen Anrufers eintragen. Wenn Anführungszeichen (“”) im dritten Feld erscheinen, wird das Passwort des Anrufers in der Passwortdatenbank des Servers gesucht.

Der Eintrag `myserver * serverpass *` enthält den PAP-Benutzernamen und das Passwort für den Einwahlserver. In Abbildung 16–3 benötigt der vertrauenswürdige Anrufer (`user2`) eine Authentifizierung von Remote-Peers. Aus diesem Grund enthält die zu `myserver` gehörende `/etc/ppp/pap-secrets`-Datei die PAP-Berechtigungsnachweise, die zu verwenden sind, wenn eine Verbindung mit `user2` hergestellt wird.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „Modifizieren der PPP-Konfigurationsdateien für PAP (Einwahlserver)“ auf Seite 481
- „Konfigurieren der PAP-Authentifizierung für vertrauenswürdige Anrufer bzw. aufrufende Programme (Hinauswahlrechner)“ auf Seite 483

Modifizieren der PPP-Konfigurationsdateien für PAP (Einwahlserver)

Die Aufgaben in diesem Abschnitt zeigen auf, wie vorhandene PPP-Konfigurationsdateien aktualisiert werden, um die PAP-Authentifizierung auf einem Einwahlserver zu unterstützen.

▼ So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)

In dem Verfahren dienen die unter „So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)“ auf Seite 468 vorgestellten PPP-Konfigurationsdateien als Beispiele.

1 Melden Sie sich als Superuser beim Einwahlserver oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie die Authentifizierungsoptionen in die `/etc/ppp/options`-Datei ein.

Sie können beispielsweise die nachstehenden fett hervorgehobenen Optionen in eine vorhandene `/etc/ppp/options`-Datei eintragen, um die PAP-Authentifizierung zu implementieren.

```
lock
auth
login
nodefaultroute
proxyarp
ms-dns 10.0.0.1
idle 120
```

`auth`	Gibt an, dass der Server den Anrufer authentifizieren muss, bevor eine Verbindung hergestellt wird.
`login`	Gibt an, dass der Remote-Anrufer durch die standardmäßigen Authentifizierungsservices für UNIX-Benutzer authentifiziert wird.
`nodefaultroute`	Gibt an, dass keine `pppd`-Sitzung auf dem lokalen System eine Standardroute ohne `root`-Berechtigungen herstellen kann.
`proxyarp`	Fügt einen Eintrag in die ARP-Tabelle (Address Resolution Protocol) des Systems ein, die die IP-Adresse des Peers und die Ethernet-Adresse des Systems angibt. Mit dieser Option ist der Peer für andere Systeme im lokalen Ethernet sichtbar.
`ms-dns 10.0.0.1`	Ermöglicht `pppd`, eine DNS-Adresse (Domain Name Server) `10.0.0.1` für den Client bereitzustellen.
`idle 120`	Gibt an, dass inaktive Benutzer nach zwei Minuten getrennt werden.

3 Fügen Sie in der `/etc/ppp/options.cua.a` -Datei die folgende Adresse für den `cua/a`-Benutzer ein:

```
:10.0.0.2
```

4 Fügen Sie in der `/etc/ppp/options.cua.b`-Datei die folgende Adresse für den `cua/b`-Benutzer ein:

```
:10.0.0.3
```

5 Fügen Sie in der `/etc/ppp/pap-secrets`-Datei den folgenden Eintrag ein:

```
*     *          ""      *
```

Hinweis – Die `login`-Option ermöglicht, wie zuvor beschrieben, die Benutzerauthentifizierung. Dieser Eintrag in der `/etc/ppp/pap-secrets` -Datei bietet die Möglichkeit, PAP standardmäßig mit der `login`-Option zu aktivieren.

Siehe auch Um PAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer des Einwahlservers zu konfigurieren, informieren Sie sich unter „Konfigurieren der PAP-Authentifizierung für vertrauenswürdige Anrufer bzw. aufrufende Programme (Hinauswahlrechner)“ auf Seite 483.

Konfigurieren der PAP-Authentifizierung für vertrauenswürdige Anrufer bzw. aufrufende Programme (Hinauswahlrechner)

Dieser Abschnitt enthält Aufgaben zum Einrichten der PAP-Authentifizierung auf Hinauswahlrechnern von vertrauenswürdigen Anrufern. Als Systemadministrator können Sie die PAP-Authentifizierung in Systemen einrichten, bevor potenzielle Anrufer authentifiziert werden. Wenn die Remote-Anrufer bereits über ihre Rechner verfügen, können Sie diesen Anrufern die in diesem Abschnitt beschriebenen Aufgaben zuweisen.

Mit dem Konfigurieren von PAP für vertrauenswürdige Anrufer sind zwei Aufgaben verbunden:

- Konfigurieren der PAP-Sicherheitsberechtigungsnachweise der Anrufer
- Konfigurieren des Hinauswahlrechners der Anrufer, um die PAP-Authentifizierung zu unterstützen

▼ So konfigurieren Sie PAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer

Dieses Verfahren zeigt, wie PAP-Berechtigungsnachweise für vertrauenswürdige Anrufer eingerichtet werden, wenn Authentifizierungs-Berechtigungsnachweise von Remote-Peers benötigt werden. Es wird vorausgesetzt, dass Sie, der Systemadministrator, die PAP-Berechtigungsnachweise auf den Hinauswahlrechnern vertrauenswürdiger Anrufer einrichten.

1 Melden Sie sich als Superuser beim Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Verwenden Sie die in Abbildung 16–3 dargestellte PAP-Beispielkonfiguration, wobei Sie davon ausgehen, dass der Hinauswahlsrechner zu `user1` gehört.

2 Modifizieren Sie die pap-secrets-Datenbank für den Anrufer.

Diese Version umfasst eine `/etc/ppp/pap-secrets`-Datei, die hilfreiche Kommentare enthält, aber keine Optionen. In diese `/etc/ppp/pap-secrets`-Datei können Sie folgende Optionen eintragen:

```
user1    myserver  pass1    *
```

Beachten Sie, dass das zu `user1` gehörende Passwort `pass1` in lesbarem ASCII-Format über die Verbindung weitergegeben wird. `myserver` ist der zu `user1` gehörende Name des Peers.

3 Melden Sie sich als Superuser bei einem anderen Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Verwenden Sie das PAP-Authentifizierungsbeispiel, wobei Sie davon ausgehen, dass der Hinauswahlrechner zu `user2` gehört.

4 Modifizieren Sie die pap-secrets-Datenbank für den Anrufer.

Am Ende der `/etc/ppp/pap-secrets`-Datei können Sie die nächsten Optionen eintragen.

```
user2     myserver   pass2       *
myserver  user2      serverpass  *
```

In diesem Beispiel hat `/etc/ppp/pap-secrets` zwei Einträge. Der erste Eintrag enthält die PAP-Sicherheitsberechtigungsnachweise, die `user2` an den Einwahlserver `myserver` zur Authentifizierung weitergibt.

`user2` benötigt PAP-Berechtigungsnachweise vom Einwahlserver, damit die Verbindung ausgehandelt werden kann. Aus diesem Grund enthält `/etc/ppp/pap-secrets` auch die PAP-Berechtigungsnachweise, die von `myserver` in der zweiten Leitung erwartet werden.

Hinweis – Da die meisten ISPs keine Authentifizierungs-Berechtigungsnachweise bereitstellen, kann das vorangegangene Szenario für die Kommunikation mit einem ISP unrealistisch erscheinen.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „So erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 480
- „So konfigurieren Sie PAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer“ auf Seite 483

Modifizieren von PPP-Konfigurationsdateien für PAP (Hinauswahlrechner)

Die folgenden Aufgaben zeigen auf, wie vorhandene PPP-Konfigurationsdateien aktualisiert werden, um die PAP-Authentifizierung auf Hinauswahlrechnern von vertrauenswürdigen Anrufern zu unterstützen.

Die folgenden Parameter werden zum Konfigurieren der PAP-Authentifizierung auf dem Hinauswahlrechner verwendet, der zu `user2` gehört, der in Abbildung 16–3 dargestellt ist. `user2` verlangt von Anrufern, sich zu authentifizieren. Dies gilt auch für Anrufe über den Einwahlserver `myserver`.

▼ So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)

In diesem Verfahren dienen die unter „So definieren Sie die Kommunikation über die serielle Verbindung“ auf Seite 460 vorgestellten PPP-Konfigurationsdateien als Beispiele. Es wird beschrieben, wie der Hinauswahlrechner konfiguriert wird, der zu `user2` gehört (siehe Abbildung 16–3).

1 Melden Sie sich beim Hinauswahlrechner als Superuser an.

2 Modifizieren Sie die `/etc/ppp/options`-Datei.

Die nächste `/etc/ppp/options`-Datei enthält die fett hervorgehobenen Optionen für die PAP-Unterstützung.

```
# cat /etc/ppp/options
lock
name user2
auth
require-pap
```

name user2 — Legt `user2` als PAP-Namen des Benutzers auf dem lokalen Rechner fest. Wenn die `login`-Option verwendet wird, muss der PAP-Name mit dem UNIX-Benutzernamen des Benutzers in der Passwortdatenbank übereinstimmen.

auth — Gibt an, dass Anrufer durch den Hinauswahlrechner authentifiziert werden müssen, bevor die Verbindung hergestellt wird.

Hinweis – Dieser Hinauswahlrechner fordert die Authentifizierung von seinen Peers an, obwohl die meisten Hinauswahlrechner keine solche Authentifizierung anfordern. Beides ist akzeptabel.

---

require-pap Fordert PAP-Berechtigungsnachweise vom Peer an.

3 Erstellen Sie im Verzeichnis `/etc/ppp/peers/` eine *peer-name*-Datei für den Remote-Rechner `myserver`.

Das nächste Beispiel zeigt, wie die PAP-Unterstützung in eine `/etc/ppp/peers/myserver` -Datei eintragen wird, die anhand des Verfahrens erstellt wurde, das unter „So definieren Sie die Verbindung mit einem bestimmten Peer“ auf Seite 462 beschrieben wird.

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user user2
remotename myserver
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

Die fett hervorgehobenen neuen Optionen dienen zum Hinzufügen von PAP-Anforderungen an den `myserver`.

user user2	Definiert `user2` als Benutzernamen für den lokalen Rechner.
remotename myserver	Definiert `myserver` als Peer, der Authentifizierungs-Berechtigungsnachweise vom lokalen Rechner benötigt.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- Um die PAP-Authentifizierung durch Aufrufen des Einwahlservers zu prüfen, informieren Sie sich unter „So rufen Sie den Einwahlserver auf“ auf Seite 469.
- Weitere Informationen zur PAP-Authentifizierung finden Sie unter „PAP (Password Authentication Protocol)“ auf Seite 549.

Konfigurieren der CHAP-Authentifizierung

Die in diesem Abschnitt enthaltenen Aufgaben zeigen, wie die Authentifizierung über eine PPP-Verbindung mithilfe des CHAP (Challenge-Handshake Authentication Protocol) implementiert wird. Das verwendete Beispiel in Abbildung 16–4 dient zur Veranschaulichung eines CHAP-Szenarios für die Einwahl in ein privates Netzwerk. Verwenden Sie die Anweisungen als Basis für die Implementierung der CLIENT-HOSTAP-Authentifizierung an Ihrem Standort.

Bevor Sie zu den nächsten Verfahren übergehen, führen Sie Folgendes aus:

- Richten Sie eine Wählverbindung zwischen dem Einwahlserver und den Hinauswahlrechnern ein, die zu vertrauenswürdigen Anrufern gehören, und testen Sie diese Wählverbindung.
- Stellen Sie eine Superuser-Berechtigung für den lokalen Rechner bereit (entweder ein Einwahlserver oder ein Hinauswahlrechner).

Einrichten der CHAP-Authentifizierung (Übersicht der Schritte)

TABELLE 19–4 Übersicht der Schritte für die CHAP-Authentifizierung (Einwahlserver)

Aufgabe	Beschreibung	Siehe
1. Zuweisung von CHAP-Geheimnissen für alle vertrauenswürdigen Anrufer	Erstellen Sie die CHAP-Geheimnisse der Anrufer, oder lassen Sie die CHAP-Geheimnisse von den Anrufern erstellen.	„So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 488
2. Erstellen der chap-secrets-Datenbank	Tragen Sie die Sicherheitsberechtigungsnachweise für alle vertrauenswürdigen Anrufer in die `/etc/ppp/chap-secrets` -Datei ein.	„So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 488
3. Modifizieren der PPP-Konfigurationsdateien	Tragen Sie die CHAP-Optionen in die Dateien `/etc/ppp/options` und `/etc/ppp/peers/`*peer-name* ein.	„So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)“ auf Seite 490

TABELLE 19–5 Übersicht der Schritte für die CHAP-Authentifizierung (Hinauswahlrechner)

Aufgabe	Beschreibung	Siehe
1. Erstellen der CHAP-Datenbank für den Rechner des vertrauenswürdigen Anrufers	Erstellen Sie die Sicherheitsberechtigungsnachweise für den vertrauenswürdigen Anrufer und bei Bedarf die Sicherheitsberechtigungsnachweise für andere Benutzer, die den Hinauswahlrechner in `/etc/ppp/chap-secrets` aufrufen.	„So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 488
2. Modifizieren der PPP-Konfigurationsdateien	Fügen Sie CHAP-Optionen in die `/etc/ppp/options`-Datei ein.	„So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)“ auf Seite 492

Konfigurieren der CHAP-Authentifizierung auf dem Einwahlserver

Der erste Schritt zum Einrichten der CHAP-Authentifizierung ist das Modifizieren der `/etc/ppp/chap-secrets`-Datei. In dieser Datei sind die CHAP-Sicherheitsberechtigungsnachweise einschließlich des CHAP-Geheimnisses enthalten, das verwendet wird, um Anrufer zu authentifizieren, die diese Verbindung verwenden.

Hinweis – UNIX- oder PAM-Authentifizierungsmechanismen funktionieren bei CHAP nicht. Sie können beispielsweise nicht die PPP-`login`-Option verwenden, die in „So erstellen Sie eine Datenbank für PAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 480 beschrieben wird. Wenn Ihr Authentifizierungsszenario die PAM- oder UNIX-basierte Authentifizierung verlangt, verwenden Sie stattdessen PAP.

Mithilfe des nächsten Verfahrens wird die CHAP-Authentifizierung für einen Einwahlserver in einem privaten Netzwerk implementiert. Die PPP-Verbindung ist die einzige Verbindung, die zur Verfügung steht. Es können nur Anrufer auf das Netzwerk zugreifen, die die entsprechenden Berechtigungen von den Administratoren des Netzwerks (oder vom Systemadministrator) erhalten haben.

▼ So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)

1 Erstellen Sie eine Liste, in der die Benutzernamen der vertrauenswürdigen Anrufer enthalten sind.

Vertrauenswürdige Anrufer sind Personen, denen die Berechtigung erteilt wurde, das private Netzwerk aufzurufen.

2 Weisen Sie jedem Benutzer ein CHAP-Geheimnis zu.

Hinweis – Verwenden Sie ein sicheres CHAP-Geheimnis, das nicht leicht erraten werden kann. Für den Inhalt des CHAP-Geheimnisses gelten keine weiteren Einschränkungen.

Die Methode der Zuweisung des CHAP-Geheimnisses unterliegt den Sicherheitsrichtlinien Ihres Standorts. Entweder sind Sie für das Erstellen von Geheimdaten verantwortlich, oder die Anrufer müssen ihre eigenen Geheimnisse erstellen. Wenn Sie nicht für die Zuweisung des CHAP-Geheimnisses verantwortlich sind, müssen Sie sicherstellen, dass Sie die CHAP-Geheimnisse erhalten, die von den vertrauenswürdigen Anrufern oder für die vertrauenswürdigen Anrufer erstellt wurden.

3. **Melden Sie sich als Superuser beim Einwahlserver oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

4. **Modifizieren Sie die `/etc/ppp/chap-secrets` -Datei.**

   Diese Version umfasst eine `/etc/ppp/chap-secrets` -Datei, die hilfreiche Kommentare enthält, aber keine Optionen. Sie können folgende Optionen für den `CallServe` am Ende der `/etc/ppp/chap-secrets`-Datei einfügen:

   ```
   account1  CallServe   key123   *
   account2  CallServe   key456   *
   ```

   `key123` ist das CHAP-Geheimnis für den vertrauenswürdigen Anrufer (`account1`).

   `key456` ist das CHAP-Geheimnis für den vertrauenswürdigen Anrufer (`account2`).

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 488
- „So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)“ auf Seite 490
- „Konfigurieren der CHAP-Authentifizierung für vertrauenswürdige Anrufer (Hinauswahlrechner)“ auf Seite 490

Modifizieren der PPP-Konfigurationsdateien für CHAP (Einwahlserver)

Die in diesem Abschnitt beschriebene Aufgabe zeigt, wie vorhandene PPP-Konfigurationsdateien aktualisiert werden, um die CHAP-Authentifizierung auf einem Einwahlserver zu unterstützen.

▼ So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)

1 **Melden Sie sich beim Einwahlserver als Superuser an.**

2 **Modifizieren Sie die `/etc/ppp/options` -Datei.**

Fügen Sie die fett hervorgehobenen Optionen für die CHAP-Unterstützung ein.

```
# cat /etc/ppp/options
lock
nodefaultroute
name CallServe
auth
```

`name` *CallServe*	Definiert *CallServe* als CHAP-Namen des Benutzers auf dem lokalen Rechner, in diesem Fall auf dem Einwahlserver.
`auth`	Veranlasst den lokalen Rechner, Anrufer zu authentifizieren, bevor eine Verbindung hergestellt wird.

3 **Erstellen Sie die übrigen PPP-Konfigurationsdateien, die zur Unterstützung der vertrauenswürdigen Anrufer dienen.**

Lesen Sie dazu „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466 und „So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)“ auf Seite 468.

Siehe auch Um CHAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer zu konfigurieren, informieren Sie sich unter „So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 488.

Konfigurieren der CHAP-Authentifizierung für vertrauenswürdige Anrufer (Hinauswahlrechner)

Dieser Abschnitt umfasst Aufgaben zum Einrichten der CHAP-Authentifizierung auf Hinauswahlrechnern von vertrauenswürdigen Anrufern. Von den Sicherheitsrichtlinien Ihres Standorts hängt ab, ob Sie oder die vertrauenswürdigen Anrufer für das Einrichten der CHAP-Authentifizierung verantwortlich sind.

Damit CHAP von Remote-Anrufern konfiguriert werden kann, müssen Sie sicherstellen, dass die lokalen CHAP-Geheimnisse der Anrufer mit den CHAP-Geheimnissen der Anrufer in der `/etc/ppp/chap-secrets`-Datei des Einwahlservers übereinstimmen. Anschließend weisen Sie den Anrufern die in diesem Abschnitt beschriebenen Aufgaben zu, damit diese CHAP konfigurieren können.

Mit dem Konfigurieren von CLIENT-HOSTAP für vertrauenswürdige Anrufer sind zwei Aufgaben verbunden:

- Erstellen der CHAP-Sicherheitsberechtigungsnachweise der Anrufer
- Konfigurieren der Hinauswahlrechner der Anrufer, um die CHAP-Authentifizierung zu unterstützen

▼ So konfigurieren Sie CHAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer

Dieses Verfahren zeigt, wie CHAP-Berechtigungsnachweise für vertrauenswürdige Anrufer eingerichtet werden. In diesem Verfahren wird vorausgesetzt, dass Sie, der Systemadministrator, die CLIENT-HOSTAP-Berechtigungsnachweise auf den Hinauswahlrechnern vertrauenswürdiger Anrufer einrichten.

1 Melden Sie sich als Superuser beim Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Verwenden Sie die in „Beispiel einer Konfiguration mit CHAP-Authentifizierung“ auf Seite 448 gezeigte CHAP-Beispielkonfiguration, wobei Sie davon ausgehen, dass der Hinauswahlrechner zu `account1` des vertrauenswürdigen Anrufers gehört.

2 Modifizieren Sie die chap-secrets-Datenbank für Anrufer `account1`.

Diese Version umfasst eine `/etc/ppp/chap-secrets`-Datei, die hilfreiche Kommentare enthält, aber keine Optionen. Sie können folgende Optionen in die `/etc/ppp/chap-secrets` -Datei einfügen:

```
account1  CallServe   key123   *
```

`CallServe` ist der Name des Peers, den `account1` zu erreichen versucht. `key123` ist das CHAP-Geheimnis, das für Verbindungen zwischen `account1` und `CallServer` verwendet wird.

3 Melden Sie sich als Superuser bei einem anderen Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Es wird vorausgesetzt, das dieser Rechner zu `account2` gehört.

4 **Modifizieren Sie die `/etc/ppp/chap-secrets` -Datenbank für Anrufer "account2".**

```
account2  CallServe   key456   *
```

Jetzt verfügt `account2` über das Geheimnis `key456`. Diese CHAP-Berechtigungsnachweise können für Verbindungen mit dem Peer `CallServe` verwendet werden.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „So erstellen Sie eine Datenbank für CHAP-Berechtigungsnachweise (Einwahlserver)“ auf Seite 488
- „So konfigurieren Sie CHAP-Authentifizierungs-Berechtigungsnachweise für vertrauenswürdige Anrufer“ auf Seite 491

Einfügen von CHAP in die Konfigurationsdateien (Hinauswahlrechner)

Weitere Informationen zur CHAP-Authentifizierung finden Sie unter „CHAP (Challenge-Handshake Authentication Protocol)“ auf Seite 552. In der nächsten Aufgabe wird beschrieben, wie der Hinauswahlrechner konfiguriert wird, der zu `account1` des Anrufers gehört. Informationen hierzu finden Sie unter „Beispiel einer Konfiguration mit CHAP-Authentifizierung“ auf Seite 448.

▼ So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)

1 **Melden Sie sich beim Hinauswahlrechner als Superuser an.**

2 **Stellen Sie sicher, dass in der `/etc/ppp/options` -Datei die folgenden Optionen enthalten sind:**

```
# cat /etc/ppp/options
lock
nodefaultroute
```

3 **Erstellen eine `/etc/ppp/peers/` *peer-name*-Datei für den Remote-Rechner `CallServe`.**

```
# cat /etc/ppp/peers/CallServe
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user account1
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

Mithilfe der Option `user account1` wird `account1` als CHAP-Benutzername festgelegt, der an `CallServe` weitergegeben wird. Eine Beschreibung der anderen Optionen in der oben genannten Datei finden Sie in derselben `/etc/ppp/peers/myserver` -Datei unter „So definieren Sie die Verbindung mit einem bestimmten Peer“ auf Seite 462.

Siehe auch Informationen zum Prüfen der CHAP-Authentifizierung durch Aufrufen des Einwahlservers finden Sie unter „So rufen Sie den Einwahlserver auf“ auf Seite 469.

◆ ◆ ◆ KAPITEL 20

Einrichten eines PPPoE-Tunnels (Aufgaben)

Dieses Kapitel enthält Aufgaben zum Einrichten der Teilnehmer an jedem Ende des PPPoE-Tunnels: PPPoE-Client und PPPoE-Zugangsserver. Folgende spezielle Themen werden behandelt:

- „Wichtige Aufgaben zum Einrichten eines PPPoE-Tunnels (Übersichten der Schritte)“ auf Seite 495
- „Einrichten des PPPoE-Clients“ auf Seite 496
- „Einrichten eines PPPoE-Zugangsservers“ auf Seite 500

In den Aufgaben wird das Szenario aufgegriffen, das unter „Planen der DSL-Unterstützung über einen PPPoE-Tunnel“ auf Seite 450 als Beispiel aufgeführt wird. Eine Übersicht zu PPPoE finden Sie unter „Unterstützung für DSL-Benutzer durch PPPoE“ auf Seite 433.

Wichtige Aufgaben zum Einrichten eines PPPoE-Tunnels (Übersichten der Schritte)

In den folgenden Tabellen werden die wichtigen Aufgaben zum Konfigurieren der PPPoE-Clients und des PPPoE-Zugangsservers aufgeführt. Um PPPoE an Ihrem Standort zu implementieren, müssen Sie nur Ihr Ende des PPPoE-Tunnels einrichten, d. h. entweder die Clientseite oder die Zugangsserverseite.

TABELLE 20–1 Übersicht der Schritte zum Einrichten eines PPPoE-Clients

Aufgabe	Beschreibung	Siehe
1. Konfigurieren einer Schnittstelle für PPPoE	Definieren Sie die Ethernet-Schnittstelle, die für den PPPoE-Tunnel verwendet werden soll.	„So konfigurieren Sie eine Schnittstelle für einen PPPoE-Client“ auf Seite 497

TABELLE 20–1 Übersicht der Schritte zum Einrichten eines PPPoE-Clients *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
2. Konfigurieren von Informationen zum PPPoE-Zugangsserver	Definieren Sie die Parameter für den Zugangsserver am Ende des Serviceproviders des PPPoE-Tunnels.	„So definieren Sie einen PPPoE-Zugangsserver-Peer“ auf Seite 498
3. Einrichten der PPP-Konfigurationsdateien	Definieren Sie die PPP-Konfigurationsdateien für den Client, falls Sie dies noch nicht getan haben.	„So definieren Sie die Kommunikation über die serielle Verbindung“ auf Seite 460
4. Erstellen des Tunnels	Rufen Sie den Zugangsserver auf.	„So definieren Sie einen PPPoE-Zugangsserver-Peer“ auf Seite 498

TABELLE 20–2 Übersicht der Schritte zum Einrichten eines PPPoE-Zugangsservers

Aufgabe	Beschreibung	Siehe
1. Einrichten eines PPPoE-Zugangsservers	Definieren Sie die Ethernet-Schnittstelle, die für den PPPoE-Tunnel verwendet werden soll, und definieren Sie die Services, die vom Zugangsserver bereitgestellt werden.	„So richten Sie einen PPPoE-Zugangsserver ein“ auf Seite 500
2. Einrichten der PPP-Konfigurationsdateien	Definieren Sie die PPP-Konfigurationsdateien für den Client, falls Sie dies noch nicht getan haben.	„Konfigurieren der Kommunikation über den Einwahlserver“ auf Seite 467
3. (Optional) Beschränken der Verwendung einer Schnittstelle	Verwenden Sie PPPoE-Optionen und die PAP-Authentifizierung, um die Verwendung einer bestimmten Ethernet-Schnittstelle auf bestimmte Clients zu beschränken.	„So beschränken Sie die Verwendung einer Schnittstelle auf bestimmte Clients“ auf Seite 501

Einrichten des PPPoE-Clients

Um PPP für Clientsysteme über DSL bereitzustellen, müssen Sie zunächst PPPoE für die Schnittstelle konfigurieren, die mit dem Modem oder Hub verbunden ist. Dann müssen Sie die PPP-Konfigurationsdateien ändern, um den Zugangsserver am anderen Ende von PPPoE zu definieren.

Voraussetzungen zum Einrichten des PPPoE-Clients

Bevor Sie den PPPoE-Client einrichten, führen Sie folgende Schritte aus:

- Installieren Sie Solaris auf den Clientrechnern, um den PPPoE-Tunnel zu verwenden.
- Kontaktieren Sie den Serviceprovider, um Informationen über dessen PPPoE-Zugangsserver zu erfragen.
- Lassen Sie von der Telefongesellschaft oder vom Serviceprovider die Geräte installieren, die von den Clientrechnern verwendet werden. Zu diesen Geräten zählen beispielsweise das DSL-Modem und der Splitter. Diese Geräte werden meist von der Telefongesellschaft installiert.

▼ So konfigurieren Sie eine Schnittstelle für einen PPPoE-Client

Wenden Sie dieses Verfahren an, um die Ethernet-Schnittstelle zu definieren, die für den PPPoE-Tunnel verwendet werden soll.

1 **Melden Sie sich als Superuser beim PPPoE-Client oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie den Namen der Ethernet-Schnittstelle mit der DSL-Verbindung in die Datei `/etc/ppp/pppoe.if` ein.**

Fügen Sie beispielsweise den folgenden Eintrag in die Datei `/etc/ppp/pppoe.if` für einen PPPoE-Client ein, der `hme0` als Netzwerkschnittstelle verwendet, die an das DSL-Modem angeschlossen ist.

```
hme0
```

Weitere Informationen zu `/etc/ppp/pppoe.if` finden Sie unter „`/etc/ppp/pppoe.if`-Datei“ auf Seite 559.

3 **Konfigurieren Sie die Schnittstelle für PPPoE.**

```
# /etc/init.d/pppd start
```

4 **(Optional) Stellen Sie sicher, dass die Schnittstelle jetzt für PPPoE angebunden ist.**

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
```

Sie können auch den Befehl `/usr/sbin/sppptun` verwenden, um die Schnittstellen für PPPoE manuell anzubinden. Die Anleitung dazu finden Sie unter „`/usr/sbin/sppptun`-Befehl“ auf Seite 560.

▼ So definieren Sie einen PPPoE-Zugangsserver-Peer

Den Zugangsserver definieren Sie in der Datei `/etc/ppp/peers/` *peer-name*. Viele der Optionen, die für den Zugangsserver verwendet werden, dienen auch zur Verwendung des Einwahlservers in einem Einwahlszenario. Eine ausführliche Beschreibung von `/etc/ppp/peers.` *peer-name* finden Sie in „`/etc/ppp/peers/` *peer-name*-Datei“ auf Seite 535.

1 **Melden Sie sich als Superuser beim PPPoE-Client oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Definieren Sie den PPPoE-Zugangsserver des Serviceproviders in der Datei `/etc/ppp/peers/`*peer-name*.**

Die folgende Datei, `/etc/ppp/peers/dslserve`, definiert beispielsweise den Zugangsserver `dslserve` von Far ISP (siehe „Beispiel einer Konfiguration für einen PPPoE-Tunnel“ auf Seite 452).

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

Eine Definition der Optionen in dieser Datei finden Sie unter „`/etc/ppp/peers/` *peer-name*-Datei zum Definieren eines Zugangsserver-Peers“ auf Seite 568.

3 **Modifizieren Sie die anderen PPP-Konfigurationsdateien auf dem PPPoE-Client.**

a. **Konfigurieren Sie `/etc/ppp/options` entsprechend den Anweisungen zum Konfigurieren eines Hinauswahlrechners unter „Konfigurieren des Hinauswahlrechners“ auf Seite 456.**

b. Erstellen Sie eine `/etc/ppp/options.sppptun`-Datei. `/etc/ppp/options.sppptun` definiert PPP-Optionen für den seriellen Port, der mit der Schnittstelle verbunden ist, die für PPPoE angebunden ist.

Sie können alle Optionen verwenden, die für die `/etc/ppp/options.` *ttyname*-Datei verfügbar sind. Diese wird in „`/etc/ppp/options.` *ttyname*-Konfigurationsdatei“ auf Seite 531 beschrieben. Sie müssen die Datei `/etc/ppp/options.sppptun` benennen, weil `sppptun` der angegebene Gerätename in der `pppd`-Konfiguration ist.

4 Stellen Sie sicher, dass alle Benutzer PPP auf dem Client starten können.

```
# touch /etc/ppp/options
```

5 Testen Sie, ob PPP über die DSL-Leitung ausgeführt werden kann.

```
% pppd debug updetach call dslserve
```

`dslserve` ist der Name, der dem Zugangsserver des ISP vergeben wird (siehe „Beispiel einer Konfiguration für einen PPPoE-Tunnel“ auf Seite 452). Die Option `debug updetach` bewirkt, dass in einem Terminalfenster Informationen zur Fehlersuche angezeigt werden.

Wenn PPP richtig ausgeführt wird, wird in der Terminalausgabe angezeigt, dass die Verbindung aktiviert wird. Wenn PPP noch nicht ausgeführt wird, verwenden Sie den folgenden Befehl, um festzustellen, ob die Server fehlerfrei ausgeführt werden:

```
# /usr/lib/inet/pppoec -i hme0
```

Hinweis – Die Benutzer von konfigurierten PPPoE-Clients können beginnen, PPP über eine DSL-Leitung auszuführen, indem sie Folgendes eingeben:

```
% pppd call ISP-server-name
```

Dann können die Benutzer eine Anwendung oder einen Service ausführen.

Siehe auch Die folgende Liste enthält Verweise auf relevante Informationen:

- „Einrichten des PPPoE-Clients“ auf Seite 496.
- „Erstellen von PPPoE-Tunneln für DSL-Unterstützung“ auf Seite 558.
- Kapitel 21, „Beheben von allgemeinen PPP-Problemen (Aufgaben)“.
- „Einrichten eines PPPoE-Zugangsservers“ auf Seite 500.

Einrichten eines PPPoE-Zugangsservers

Wenn Ihr Unternehmen ein Serviceprovider ist, können Sie Ihren Kunden, die über DSL Zugriff auf Ihre Site haben, Internetservices und andere Services anbieten. Dazu müssen Sie die Serverschnittstellen für den PPPoE-Tunnel definieren und festlegen, welche Services den Benutzern zur Verfügung gestellt werden.

▼ So richten Sie einen PPPoE-Zugangsserver ein

Wenden Sie dieses Verfahren an, um die Ethernet-Schnittstelle zu definieren, die für den PPPoE-Tunnel verwendet werden soll, und konfigurieren Sie die Services, die vom Zugangsserver bereitgestellt werden.

1 **Melden Sie sich als Superuser beim Zugangsserver oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie den Namen der Ethernet-Schnittstellen, die für die PPPoE-Tunnel bestimmt sind, in die Datei `/etc/ppp/pppoe.if` ein.**

Sie würden beispielsweise die folgende Datei `/etc/ppp/pppoe.if` für den Zugangsserver `dslserve` verwenden, der unter „Beispiel einer Konfiguration für einen PPPoE-Tunnel“ auf Seite 452 angezeigt wird.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
```

3 **Definieren Sie die globalen Services, die vom Zugangsserver in der Datei `/etc/ppp/pppoe` bereitgestellt werden.**

Die folgende `/etc/ppp/pppoe`-Datei dient zum Auflisten der Services, die vom Zugangsserver `dslserve` bereitgestellt werden (siehe Abbildung 16–5).

```
device hme1,hme2
service internet
    pppd "proxyarp 192.168.1.1:"
service debugging
    pppd "debug proxyarp 192.168.1.1:"
```

In der Beispieldatei wird ein Internetservice für die Ethernet-Schnittstellen von `dslserve` (`hme1` und `hme2`) angekündigt. Die Fehlersuche für PPP-Verbindungen wird über die Ethernet-Schnittstellen aktiviert.

4. **Richten Sie die PPP-Konfigurationsdateien auf die gleiche Weise ein, wie Sie es für einen Einwahlserver tun würden.**

   Weitere Informationen finden Sie unter „Erstellen eines IP-Adressierungsschemas für Anrufer“ auf Seite 556.

5. **Starten Sie den `pppoed`-Dämon.**

   ```
   # /etc/init.d/pppd start
   ```

   `pppd` dient zudem zum Anbinden der Schnittstellen, die in `/etc/ppp/pppoe.if` aufgeführt sind.

6. **(Optional) Stellen Sie sicher, dass die Serverschnittstellen für PPPoE angebunden sind.**

   ```
   # /usr/sbin/sppptun query
   hme1:pppoe
   hme1:pppoed
   hme2:pppoe
   hme2:pppoed
   ```

   Im vorangegangenen Beispiel ist zu sehen, dass die Schnittstellen `hme1` und `hme2` derzeit für PPPoE angebunden sind. Sie können auch den Befehl `/usr/sbin/sppptun` verwenden, um die Schnittstellen für PPPoE manuell anzubinden. Die Anleitung dazu finden Sie unter „`/usr/sbin/sppptun`-Befehl“ auf Seite 560.

▼ So modifizieren Sie eine `/etc/ppp/pppoe` -Datei

1. **Melden Sie sich als Superuser beim Zugangsserver oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Modifizieren Sie nach Bedarf `/etc/ppp/pppoe`.**

3. **Führen Sie die nötigen Schritte aus, damit der `pppoed`-Dämon die neuen Services erkennt.**

   ```
   # pkill -HUP pppoed
   ```

▼ So beschränken Sie die Verwendung einer Schnittstelle auf bestimmte Clients

Das nächste Verfahren zeigt, wie eine Schnittstelle auf eine Gruppe von PPPoE-Clients beschränkt wird. Bevor Sie diese Aufgabe planen, müssen Sie die Ethernet-MAC-Adressen der Clients bereitstellen, die Sie der Schnittstelle zuweisen.

Hinweis – Auf manchen Systemen ist es möglich, die MAC-Adresse der Ethernet-Schnittstelle zu ändern. Dies ist zwar bequem, aber dient nicht der Sicherheit.

Diese Schritte zeigen anhand des unter „Beispiel einer Konfiguration für einen PPPoE-Tunnel“ auf Seite 452 aufgeführten Beispiels, wie eine der Schnittstellen von `dslserve`, in diesem Falle `hme1`, für Clients von MiddleCo verwendet wird.

1 **Konfigurieren Sie die Schnittstellen des Zugangsservers, und definieren Sie die Services. Informationen zur Vorgehensweise finden Sie unter „So richten Sie einen PPPoE-Zugangsserver ein“ auf Seite 500.**

2 **Erstellen Sie Einträge für die Clients in der `/etc/ethers`-Datenbank des Servers.**

Es folgt ein Beispieleintrag für die Clients Red, Blue und Yellow.

```
8:0:20:1:40:30 redether
8:0:20:1:40:10 yellowether
8:0:20:1:40:25 blueether
```

In dem Beispiel werden die symbolischen Namen `redether`, `yellowether` und `blueether` den Ethernet-Adressen der Clients Red, Yellow und Blue zugewiesen. Die Zuweisung von symbolischen Namen zu MAC-Adressen ist optional.

3 **Beschränken Sie die über eine bestimmte Schnittstelle bereitgestellten Services, indem Sie die folgenden Informationen in der `/etc/ppp/pppoe.`*device*-Datei definieren.**

In der Datei ist *device* der Name des Geräts, das definiert werden soll.

```
# cat /etc/ppp/pppoe.hme1
service internet
     pppd "name dslserve-hme1"
     clients redether,yellowether,blueether
```

`dslserve-hme1` ist der Name des Zugangsservers, der für den Abgleich der Einträge verwendet wird, die in der `pap-secrets`-Datei vorhanden sind. Die Option `clients` dient zum Beschränken der Verwendung der Schnittstelle `hme1` auf Clients mit den symbolischen Ethernetnamen `redether`, `yellowether` und `blueether`.

Wenn Sie keine symbolischen Namen für die MAC-Adressen des Clients in `/etc/ethers` definieren, können Sie die numerischen Adressen als Argumente für die `clients`-Option verwenden. Platzhalterzeichen sind zulässig.

Sie können beispielsweise die numerische Adresse `clients 8:0:20:*:*:*` angeben. Wenn Sie Platzhalterzeichen verwenden, werden alle übereinstimmenden Adressen in `/etc/ethers` akzeptiert.

4 **Erstellen Sie die `/etc/ppp/pap-secrets`-Datei für den Zugangsserver:**

```
Red         dslserve-hme1   redpasswd     *
Blue        dslserve-hme1   bluepasswd    *
Yellow      dslserve-hme1   yellowpassd   *
```

Die Einträge sind die PAP-Namen und Passwörter der Clients, die PPP über die Schnittstelle `hme1` von `dslserve` ausführen können.

Weitere Informationen zur PAP-Authentifizierung finden Sie unter „Konfigurieren der PAP-Authentifizierung“ auf Seite 478.

Siehe auch Es folgen Verweise auf relevante Informationen:

- Weitere Informationen zu PPPoE finden Sie unter „Erstellen von PPPoE-Tunneln für DSL-Unterstützung“ auf Seite 558.
- Informationen zur Fehlerbehebung bei Problemen mit PPPoE und PPP finden Sie unter „Lösen von Problemen im Zusammenhang mit PPP und PPPoE“ auf Seite 509.
- Informationen zum Konfigurieren eines PPPoE-Clients finden Sie unter „Einrichten des PPPoE-Clients“ auf Seite 496.
- Informationen zum Konfigurieren der PAP-Authentifizierung für einen Client finden Sie unter „Konfigurieren der PAP-Authentifizierung für vertrauenswürdige Anrufer bzw. aufrufende Programme (Hinauswahlrechner)“ auf Seite 483.
- Informationen zum Konfigurieren der PAP-Authentifizierung auf einem Server finden Sie unter „Konfigurieren der PAP-Authentifizierung auf dem Einwahlserver“ auf Seite 479.

◆ ◆ ◆ KAPITEL 21

Beheben von allgemeinen PPP-Problemen (Aufgaben)

Dieses Kapitel enthält Informationen zur Behebung von allgemeinen Problemen mit Solaris PPP 4.0. Folgende Themen werden behandelt:

- „Tools zur Behebung von PPP-Problemen“ auf Seite 506
- „Lösen von Problemen im Zusammenhang mit PPP und PPPoE“ auf Seite 509
- „Beheben von Standleitungsproblemen“ auf Seite 523
- „Diagnostizieren und Beheben von Authentifizierungsproblemen “ auf Seite 523

Unter *PPP Design, Implementation, and Debugging* von James Carlson und auf der Website der Australian National University sind ebenfalls ausführliche Informationen zur PPP-Fehlerbehebung zu finden. Weitere Informationen finden Sie unter „Professionelle Referenzpublikationen über PPP“ auf Seite 424 und „Websites über PPP“ auf Seite 424.

Lösen von PPP-Problemen (Übersicht der Schritte)

Die folgende Übersicht der Schritte umfasst Empfehlungen und Lösungen für allgemeine PPP-Probleme.

TABELLE 21–1 Übersicht der Schritte für die PPP-Fehlerbehebung

Aufgabe	Definition	Siehe
Abrufen von Diagnoseinformationen zur PPP-Verbindung	Verwenden Sie die PPP-Diagnosetools, um Informationen zur Fehlerbehebung zu erhalten.	„So rufen Sie Diagnoseinformationen aus `pppd` ab“ auf Seite 507
Abrufen von Informationen zur Fehlersuche bei einer PPP-Verbindung	Führen Sie den Befehl `pppd debug` aus, um Informationen zur Fehlerbehebung zu generieren.	„So aktivieren Sie die PPP-Fehlersuche“ auf Seite 508

TABELLE 21–1 Übersicht der Schritte für die PPP-Fehlerbehebung *(Fortsetzung)*

Aufgabe	Definition	Siehe
Behebung von allgemeinen Problemen, die das Netzwerk betreffen	Lokalisieren und beheben Sie netzwerkbezogene PPP-Probleme, indem Sie eine Reihe von Prüfungen durchführen.	„So diagnostizieren Sie Netzwerkprobleme“ auf Seite 510
Fehlerbehebung bei allgemeinen Kommunikationsproblemen	Lokalisieren und beheben Sie Kommunikationsprobleme, die die PPP-Verbindung betreffen.	„So diagnostizieren und beheben Sie Kommunikationsprobleme“ auf Seite 512
Fehlerbehebung bei Konfigurationsproblemen	Lokalisieren und beheben Sie Probleme, von denen die PPP-Konfigurationsdateien betroffen sind.	„So diagnostizieren Sie Probleme mit der PPP-Konfiguration“ auf Seite 514
Beheben von Modemproblemen	Lokalisieren und beheben Sie Modemprobleme.	„So diagnostizieren Sie Modemprobleme“ auf Seite 515
Beheben von Chat-Skript-Problemen	Lokalisieren und beheben Sie Chat-Skript-Probleme, die einen Hinauswahlrechner betreffen.	„So rufen Sie Informationen zur Fehlersuche für Chat-Skripten ab“ auf Seite 516
Beheben von Problemen mit der Übertragungsrate der seriellen Verbindung	Lokalisieren und beheben Sie Probleme mit der Übertragungsrate der seriellen Verbindung, die einen Einwahlserver betreffen.	„So diagnostizieren und beheben Sie Probleme im Zusammenhang mit der Übertragungsrate einer seriellen Verbindung“ auf Seite 519
Behebung von allgemeinen Problemen, die Standleitungen betreffen	Lokalisieren und beheben Sie Probleme, die die Leistung einer Standleitung betreffen.	„Beheben von Standleitungsproblemen“ auf Seite 523
Behebung von Authentifizierungsproblemen	Lokalisieren und beheben Sie Probleme im Zusammenhang mit Authentifizierungsdatenbanken.	„Diagnostizieren und Beheben von Authentifizierungsproblemen “ auf Seite 523
Fehlerbehebung in PPPoE-Problembereichen	Verwenden Sie die PPP-Diagnosetools, um Informationen zur Lokalisierung und Behebung von PPPoE-Problemen zu erhalten.	„So rufen Sie Diagnoseinformationen für PPPoE ab“ auf Seite 520

Tools zur Behebung von PPP-Problemen

Bei PPP-Verbindungen treten die folgenden drei Fehler auf:

- Fehler beim Herstellen einer Verbindung
- Schlechte Verbindung bei regulärer Verwendung

- Probleme, die auf die Netzwerke an beiden Seiten der Verbindung zurückzuführen sind

Die einfachste Möglichkeit, um festzustellen, ob PPP fehlerfrei funktioniert, besteht darin, einen Befehl über die Verbindung auszuführen. Senden Sie einen Befehl wie `ping` oder `traceroute` an einen Host im Netzwerk des Peers. Anschließend prüfen Sie die Ergebnisse. Um die Leistung einer bestehenden Verbindung zu überwachen oder Fehler an einer Verbindung zu beheben, sollten Sie PPP- und UNIX-Fehlerbehebungstools verwenden.

In diesem Abschnitt wird beschrieben, wie Diagnoseinformationen aus `pppd` und den zugehörigen Protokolldateien abgerufen werden. In den übrigen Abschnitten dieses Kapitels werden allgemeine PPP-Probleme beschrieben, die Sie mithilfe der PPP-Fehlerbehebungtools lokalisieren und beheben können.

So rufen Sie Diagnoseinformationen aus `pppd` ab

Anhand des folgenden Verfahrens wird demonstriert, wie die aktuellen Vorgänge einer Verbindung auf dem lokalen Rechner angezeigt werden.

1. **Melden Sie sich als Superuser beim lokalen Rechner oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Führen Sie `pppd` aus, wobei das serielle Gerät als Argument für PPP konfiguriert sein muss:**

   ```
   # pppd cua/b debug updetach
   ```

   Im folgenden Beispiel werden die resultierenden Ausgaben für eine Wählverbindung und eine Standleitungsverbindung gezeigt, wenn `pppd` im Vordergrund ausgeführt wird. Wenn Sie `pppd debug` im Hintergrund ausführen, wird die resultierende Ausgabe an die `/etc/ppp/connect-errors`-Datei gesendet.

Beispiel 21–1 Ausgabe, die aus einer funktionierenden Wählverbindung resultiert

```
# pppd /dev/cua/b debug updetach
have route to 0.0.0.0/0.0.0.0 via 172.21.0.4
serial speed set to 230400 bps
Using interface sppp0
Connect: sppp0 <--> /dev/cua/b
sent [LCP ConfReq id=0x7b <asyncmap 0x0> <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP Ident id=0x79 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6
    2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
    rcvd [LCP ConfRej id=0x7b <asyncmap 0x0>]
sent [LCP Ident id=0x7c magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Sep 15
    2004 09:38:33)"
sent [LCP ConfReq id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
```

```
rcvd [LCP ConfAck id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP Ident id=0x7e magic=0x73e981c8 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Sep 15 2004 09:38:33)"]
sent [IPCP ConfReq id=0x3d <addr 0.0.0.0> <compress VJ 0f 01>]
rcvd [LCP Ident id=0x7a magic=0xdd4ad820 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Oct  6 2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
rcvd [IPCP ConfReq id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
sent [IPCP ConfAck id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
rcvd [IPCP ConfNak id=0x3d <addr 10.0.0.2>]]
sent [IPCP ConfReq id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [IPCP ConfAck id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

Beispiel 21–2 Ausgabe, die aus einer funktionierenden Standleitungsverbindung resultiert

```
# pppd /dev/se_hdlc1 default-asyncmap debug updetach
pppd 2.4.0b1 (Sun Microsystems, Inc., Oct 24 2004 07:13:18) started by root, uid 0
synchronous speed appears to be 0 bps
init option: '/etc/ppp/peers/syncinit.sh' started (pid 105122)
Serial port initialized.
synchronous speed appears to be 64000 bps
Using interface sppp0
Connect: sppp0 <--> /dev/se_hdlc1
sent [LCP ConfReq id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfAck id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP Ident id=0xea magic=0x474283c6 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
sent [IPCP ConfReq id=0xf7 <addr 0.0.0.0> <compress VJ Of o1>]]
sent [CCP ConfReq id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [LCP Ident id=0x23 magic=0x8e3a53ff "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 22 2004 14:31:44)
rcvd [IPCP ConfReq id=0x25 <addr 10.0.0.1> <compress VJ Of 01>]
sent [IPCP ConfAck id=0x25 <addr 10.0.0.1> <compress VJ Of 01>]
rcvd [CCP ConfReq id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
sent [CCP ConfAck id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
rcvd [IPCP ConfNak id=0xf8 <addr 10.0.0.2>]
rcvd [IPCP ConfReq id=0xf7 <addr 10.0.0.2> <compress VJ Of 01>]
rcvd [CCP ConfAck id=0x3f <deflate 15> <deflate(old#) 15 <bsd v1 15>]
Deflate (15) compression enabled
rcvd [IPCP ConfAck id=0xf8 <addr 10.0.0.2> <compress VJ Of 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

▼ So aktivieren Sie die PPP-Fehlersuche

In der folgenden Aufgabe wird gezeigt, wie der `pppd`-Befehl zu verwenden ist, um Informationen zur Fehlersuche abzurufen.

Hinweis – Sie müssen für jeden Host jeweils nur einmal die Schritte 1 bis 3 ausführen. Anschließend fahren Sie mit Schritt 4 fort, um die Fehlersuche für den Host zu aktivieren.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erstellen Sie eine Protokolldatei, um die Ausgabe von `pppd` zu erfassen.**

   ```
   # touch /var/log/pppdebug
   ```

3. **Fügen Sie die folgenden `syslog`-Funktionen für `pppd` in `/etc/syslog.conf` ein.**

   ```
   daemon.debug;local2.debug       /var/log/pppdebug
   ```

4. **Führen Sie einen Neustart von `syslogd` aus.**

   ```
   # pkill -HUP -x syslogd
   ```

5. **Aktivieren Sie die Fehlersuche für Aufrufe, die an einen bestimmten Peer gesendet werden, indem Sie die folgende Syntax von `pppd` verwenden:**

   ```
   # pppd debug call peer-name
   ```

   peer-name muss der Name einer Datei im `/etc/ppp/peers`-Verzeichnis sein.

6. **Zeigen Sie den Inhalt der Protokolldatei an.**

   ```
   # tail -f /var/log/pppdebug
   ```

   Ein Beispiel für eine Protokolldatei finden Sie in Schritt 3.

Lösen von Problemen im Zusammenhang mit PPP und PPPoE

In den folgenden Abschnitten finden Sie Informationen zum Lösen von Problemen im Zusammenhang mit PPP und PPPoE.

- „So diagnostizieren Sie Netzwerkprobleme“ auf Seite 510
- „Allgemeine Netzwerkprobleme, von denen PPP betroffen ist“ auf Seite 512
- „So diagnostizieren und beheben Sie Kommunikationsprobleme“ auf Seite 512
- „Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist“ auf Seite 513
- „So diagnostizieren Sie Probleme mit der PPP-Konfiguration“ auf Seite 514
- „Allgemeine PPP-Konfigurationsprobleme“ auf Seite 515
- „So diagnostizieren Sie Modemprobleme“ auf Seite 515
- „So rufen Sie Informationen zur Fehlersuche für Chat-Skripten ab“ auf Seite 516
- „Allgemeine Chat-Skript-Probleme“ auf Seite 517
- „So diagnostizieren und beheben Sie Probleme im Zusammenhang mit der Übertragungsrate einer seriellen Verbindung“ auf Seite 519

- „So rufen Sie Diagnoseinformationen für PPPoE ab“ auf Seite 520

So diagnostizieren Sie Netzwerkprobleme

Wenn die PPP-Verbindung aktiviert ist, aber nur wenige Hosts im Remote-Netzwerk erreichbar sind, kann ein Netzwerkproblem vorliegen. Anhand des folgenden Verfahrens wird demonstriert, wie Netzwerkprobleme isoliert und beseitigt werden, die sich auf eine PPP-Verbindung auswirken.

1. **Melden Sie sich als Superuser beim lokalen Rechner oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Beenden Sie die fehlerhafte Verbindung.**

3. **Deaktivieren Sie die optionalen Protokolle in den Konfigurationsdateien, indem Sie die folgenden Optionen in Ihre PPP-Konfiguration einfügen:**

   ```
   noccp novj nopcomp noaccomp default-asyncmap
   ```

   Diese Optionen dienen zum Bereitstellen des einfachsten unkomprimierten PPP, das verfügbar ist. Versuchen Sie, diese Optionen als Argumente für `pppd` in der Befehlszeile aufzurufen. Wenn Sie einen der nicht erreichbaren Hosts erreichen, fügen Sie die Optionen an einer der folgenden Stellen ein:

   - `/etc/ppp/peers/`*peer-name*, nach der `call`-Option
   - `/etc/ppp/options`, um sicherzustellen, dass die Optionen global wirksam werden

4. **Rufen Sie den Remote-Peer auf. Aktivieren Sie dann die Fehlersuche.**

   ```
   % pppd debug call peer-name
   ```

5. **Rufen Sie ausführliche Protokolle aus dem Chat-Programm auf, indem Sie die `-v`-Option von `chat` verwenden.**

   Verwenden Sie beispielsweise in einer PPP-Konfigurationsdatei das folgende Format:

   ```
   connect 'chat -v -f /etc/ppp/chatfile'
   ```

   /etc/ppp/chatfile stellt den Namen Ihrer Chat-Datei dar.

6. **Versuchen Sie, das Problem zu reproduzieren, indem Sie Telnet oder eine andere Anwendung verwenden, um die Remote-Hosts zu erreichen.**

   Prüfen Sie die Fehlersuchprotokolle. Wenn Sie weiterhin keine Remote-Hosts erreichen können, handelt es sich bei dem PPP-Problem möglicherweise um ein Netzwerkproblem.

7 **Stellen Sie sicher, dass die IP-Adressen der Remote-Hosts registrierte Internetadressen sind.**

In manchen Organisationen werden interne IP-Adressen zugewiesen, die innerhalb des lokalen Netzwerks bekannt sind, aber nicht zum Internet weitergeleitet werden können. Wenn die Remote-Hosts sich innerhalb Ihres Unternehmens befinden, müssen Sie einen NAT-Server (Name-to-Address Translation) oder Proxyserver einrichten, um Zugang zum Internet zu erhalten. Wenn sich die Remote-Hosts nicht in Ihrem Unternehmen befinden, sollten Sie die betreffende externe Organisation von dem Problem in Kenntnis setzen.

8 **Prüfen Sie die Routing-Tabellen.**

a. **Prüfen Sie die Routing-Tabellen sowohl auf dem lokalen Rechner als auch auf dem Peer.**

b. **Stellen Sie anhand der Routing-Tabellen fest, ob Router auf dem Pfad vorhanden sind, der vom Peer zum Remote-System führt. Stellen Sie zudem fest, ob Router auf dem Pfad vorhanden sind, der zurück zum Peer führt.**

Stellen Sie sicher, dass die zwischengeschalteten Router richtig konfiguriert sind. Oft ist das Problem auf dem Pfad zu finden, der zum Peer zurück führt.

9 **(Optional) Wenn der Rechner ein Router ist, prüfen Sie die optionalen Funktionen.**

```
# ndd -set /dev/ip ip_forwarding 1
```

Weitere Informationen zu ndd finden Sie auf der Manpage ndd(1M).

In Solaris 10 können Sie routeadm(1M) anstelle von ndd(1M) verwenden.

```
# routeadm -e ipv4-forwarding -u
```

Hinweis – Der ndd-Befehl ist kein Dauerbefehl. Die mit diesem Befehl festgelegten Werte werden unwirksam, wenn das System neu gestartet wird. Der routeadm -Befehl ist ein Dauerbefehl. Die mit diesem Befehl festgelegten Werte bleiben wirksam, wenn das System neu gestartet wird.

---

10 **Prüfen Sie die Statistiken, die mit `netstat -s` und ähnlichen Tools bereitgestellt werden.**

Umfassende Informationen zu netstat finden Sie auf der Manpage netstat(1M).

a. **Erstellen Sie Statistiken auf dem lokalen Rechner.**

b. **Rufen Sie den Peer auf.**

c. **Prüfen Sie die neuen Statistiken, die mit `netstat -s` bereitgestellt wurden. Weitere Informationen finden Sie unter „Allgemeine Netzwerkprobleme, von denen PPP betroffen ist“ auf Seite 512.**

11 Prüfen Sie die DNS-Konfiguration.

Eine fehlerhafte Name Service-Konfiguration führt zum Ausfall von Anwendungen, da die IP-Adressen nicht aufgelöst werden können.

Allgemeine Netzwerkprobleme, von denen PPP betroffen ist

Sie können die von `netstat -s` erzeugten Meldungen verwenden, um die Netzwerkprobleme zu beheben, die in der folgenden Tabelle aufgeführt sind. Weitere Informationen zur Verfahrensweise finden Sie unter „So diagnostizieren Sie Netzwerkprobleme“ auf Seite 510.

TABELLE 21–2 Allgemeine Netzwerkprobleme, von denen PPP betroffen ist

Meldung	Problem	Lösung
`IP packets not forwardable`	Es ist keine Route für den lokalen Host vorhanden.	Fügen Sie die fehlende Route der Routing-Tabelle des lokalen Hosts hinzu.
`ICMP input destination unreachable`	Es ist keine Route für den lokalen Host vorhanden.	Fügen Sie die fehlende Route der Routing-Tabelle des lokalen Hosts hinzu.
`ICMP time exceeded`	Zwei Router senden sich dieselbe Zieladresse zu, wodurch das Paket hin und her geht, bis der Lebensdauerwert (Time-To-Live, TTL) überschritten ist.	Verwenden Sie `traceroute`, um die Quelle der Routing-Schleife zu lokalisieren. Benachrichtigen Sie anschließend den Administrator über den fehlerhaften Router. Informationen zu `traceroute` finden Sie auf der Manpage `traceroute(1M)`.
`IP packets not forwardable`	Es ist keine Route für den lokalen Host vorhanden.	Fügen Sie die fehlende Route der Routing-Tabelle des lokalen Hosts hinzu.
`ICMP input destination unreachable`	Es ist keine Route für den lokalen Host vorhanden.	Fügen Sie die fehlende Route der Routing-Tabelle des lokalen Hosts hinzu.

▼ So diagnostizieren und beheben Sie Kommunikationsprobleme

Es treten Kommunikationsprobleme auf, wenn zwei Peers keine Verbindung herstellen können. Manchmal handelt es sich bei diesen Problemen um Aushandlungsprobleme, die auf falsch konfigurierte Chat-Skripten zurückzuführen sind. Das folgende Verfahren zeigt, wie Sie Kommunikationsprobleme beseitigen. Informationen zum Beseitigen von Aushandlungsproblemen, die auf ein fehlerhaftes Chat-Skript zurückzuführen sind, finden Sie in Tabelle 21–5.

1. **Melden Sie sich als Superuser beim lokalen Rechner oder als Benutzer mit einer entsprechenden Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Rufen Sie den Peer auf.**

3. **Rufen Sie den Remote-Peer auf. Aktivieren Sie dann die Fehlersuche.**

   ```
   % pppd debug call peer-name
   ```

   Sie können Informationen zur Fehlersuche vom Peer abrufen, um bestimmte Kommunikationsprobleme zu beseitigen.

4. **Prüfen Sie die resultierenden Protokolle auf Kommunikationsprobleme. Weitere Informationen finden Sie unter „Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist“ auf Seite 513.**

Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist

In der folgenden Tabelle werden Symptome aufgeführt, die mit der Protokollausgabe des unter „So diagnostizieren und beheben Sie Kommunikationsprobleme“ auf Seite 512 beschriebenen Verfahrens zusammenhängen.

TABELLE 21–3 Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist

Symptom	Problem	Lösung
`too many Configure-Requests`	Ein Peer kann keine Signale vom anderen Peer empfangen.	Prüfen Sie, ob eines der folgenden Probleme vorliegt: ■ Die Verkabelung des Rechners oder der Modems kann fehlerhaft sein. ■ Die Bit-Einstellungen der Modemkonfiguration können falsch sein. Die Flusskontrolle der Konfiguration könnte unterbrochen sein. ■ Das Chat-Skript könnte fehlgeschlagen haben. Entnehmen Sie in diesem Fall die erforderlichen Informationen aus Tabelle 21–5.

TABELLE 21–3 Allgemeine Kommunikationsprobleme, von denen PPP betroffen ist *(Fortsetzung)*

Symptom	Problem	Lösung
Die `pppd debug`-Ausgabe zeigt, dass LCP gestartet wird. Jedoch schlagen die Protokolle auf der höheren Ebene fehl oder zeigen CRC-Fehler an.	Die Map für asynchrone Steuerzeichen (Asynchronous Control Character Map, ACCM) ist falsch eingerichtet.	Verwenden Sie die `default-async`-Option, um die ACCM auf die Standardeinstellung FFFFFFFF zu setzen. Versuchen Sie zunächst, `default-async` als Option für `pppd` in der Befehlszeile zu verwenden. Wenn das Problem nicht mehr besteht, fügen Sie `default-async` in `/etc/ppp/options` oder in `/etc/ppp/peers/`*peer-name* hinter der Aufrufoption ein.
Die `pppd debug`-Ausgabe zeigt, dass IPCP gestartet, aber dann sofort beendet wird.	IP-Adressen können falsch konfiguriert sein.	1. Prüfen Sie das Chat-Skript, um festzustellen, ob im Skript falsche IP-Adressen enthalten sind. 2. Wenn das Chat-Skript fehlerfrei ist, fordern Sie Fehlersuchprotokolle für den Peer an und prüfen die IP-Adressen in den Peer-Protokollen.
Die Verbindung ist sehr leistungsschwach.	Das Modem könnte falsch konfiguriert sein. Dies kann auf Fehler in der Konfiguration der Verkehrssteuerung, Modemeinrichtungsfehler oder falsch konfigurierte DTE-Übertragungsraten zurückzuführen sein.	Prüfen Sie die Modemkonfiguration. Korrigieren Sie bei Bedarf die Konfiguration.

▼ So diagnostizieren Sie Probleme mit der PPP-Konfiguration

Manche PPP-Probleme können auf Probleme in den PPP-Konfigurationsdateien zurückgeführt werden. Anhand des folgenden Verfahrens wird demonstriert, wie Sie allgemeine Konfigurationsprobleme isolieren und beseitigen.

1 Melden Sie sich als Superuser beim lokalen Rechner oder als Benutzer mit einer entsprechenden Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Rufen Sie den Remote-Peer auf. Aktivieren Sie dann die Fehlersuche.

```
% pppd debug call peer-name
```

3 Prüfen Sie das resultierende Protokoll auf Konfigurationsprobleme. Weitere Informationen finden Sie unter „Allgemeine PPP-Konfigurationsprobleme“ auf Seite 515.

Allgemeine PPP-Konfigurationsprobleme

In der folgenden Tabelle werden Symptome aufgeführt, die mit der Protokollausgabe des unter „So diagnostizieren Sie Probleme mit der PPP-Konfiguration“ auf Seite 514 beschriebenen Verfahrens zusammenhängen.

TABELLE 21–4 Allgemeine PPP-Konfigurationsprobleme

Symptom	Problem	Lösung
Die `pppd debug`-Ausgabe enthält die Fehlermeldung `Could not determine remote IP address` (Remote-IP-Adresse konnte nicht bestimmt werden).	In der `/etc/ppp/peers/`*peer-name*-Datei ist keine IP-Adresse für den Peer enthalten. Der Peer stellt während der Aushandlung der Verbindung keine IP-Adresse bereit.	Stellen Sie in der pppd-Befehlszeile oder in `/etc/ppp/peers/`*peer-name* eine IP-Adresse für den Peer bereit, indem Sie das folgende Format verwenden: :10.0.0.10
Die `pppd debug`-Ausgabe zeigt an, dass die CCP-Datenkomprimierung nicht durchgeführt werden konnte. Die Ausgabe zeigt außerdem an, dass die Verbindung abgebrochen wurde.	Die PPP-Komprimierungskonfigurationen der Peers können miteinander in Konflikt stehen.	Deaktivieren Sie die CCP-Komprimierung, indem Sie die `noccp`-Option in `/etc/ppp/options` für einen der Peers einfügen.

▼ So diagnostizieren Sie Modemprobleme

Ein Modem kann ein Hauptproblembereich für eine Wählverbindung sein. Eines der häufigsten Anzeichen für Probleme mit der Modemkonfiguration ist die ausbleibende Antwort vom Peer. Die Vorgehensweise kann sich jedoch schwierig gestalten, wenn ein Verbindungsproblem tatsächlich auf die Modemkonfiguration zurückzuführen ist.

Empfehlungen zur Beseitigung grundlegender Modemprobleme finden Sie unter „Troubleshooting Terminal and Modem Problems“ in *System Administration Guide: Advanced Administration*. In der Dokumentation des Modemherstellers und auf entsprechenden Websites sind Lösungen für Probleme sowie die dafür erforderlichen speziellen Geräte zu finden. Anhand des folgenden Verfahrens kann festgestellt werden, ob Verbindungsprobleme auf eine fehlerhafte Modemkonfiguration zurückzuführen sind.

1. **Rufen Sie den Peer bei aktivierter Fehlersuche auf (siehe „So aktivieren Sie die PPP-Fehlersuche“ auf Seite 508).**

2. **Zeigen Sie das resultierende `/var/log/pppdebug` -Protokoll an, um festzustellen, ob das Problem auf eine fehlerhafte Modemkonfiguration zurückzuführen ist.**

3 **Verwenden Sie `ping` verwenden, um Pakete unterschiedlicher Größe über die Verbindung zu senden.**

Ausführliche Informationen zu `ping` finden Sie auf der Manpage `ping(1M)`.

Wenn kleine Pakete empfangen aber größere Pakete abgeworfen werden, liegen möglicherweise Modemprobleme vor.

4 **Prüfen Sie die Schnittstelle `sppp0` auf Fehler:**

```
% netstat -ni
Name  Mtu  Net/Dest   Address      Ipkts    Ierrs Opkts    Oerrs Collis Queue
lo0   8232 127.0.0.0  127.0.0.1    826808   0     826808   0     0      0
hme0  1500 172.21.0.0 172.21.3.228 13800032 0     1648464  0     0      0
sppp0 1500 10.0.0.2   10.0.0.1     210      0     128      0     0      0
```

Wenn mit der Zeit immer mehr Schnittstellenfehler auftreten, ist die Modemkonfiguration unter Umständen falsch.

Allgemeine Fehler

Wenn Sie das `/var/log/pppdebug`-Protokoll anzeigen, können die folgenden Symptome in der Ausgabe auf eine fehlerhafte Modemkonfiguration hindeuten. Der lokale Rechner kann Signale vom Peer empfangen, aber der Peer kann keine Signale vom lokalen Rechner empfangen.

- Vom Peer sind keine `recvd`-Meldungen eingegangen.
- In der Ausgabe sind LCP-Meldungen vom Peer enthalten, aber es kommen zu viele `too many LCP Configure Requests`-Meldungen vom lokalen Rechner und die Verbindung kann nicht hergestellt werden.
- Die Verbindung wird mit einem SIGHUP-Signal abgebrochen.

▼ So rufen Sie Informationen zur Fehlersuche für Chat-Skripten ab

Wenden Sie das folgende Verfahren an, um Informationen zur Fehlersuche aus `chat` sowie Empfehlungen zur Beseitigung von allgemeinen Problemen abzurufen. Weitere Informationen finden Sie unter „Allgemeine Chat-Skript-Probleme“ auf Seite 517.

1 **Melden Sie sich als Superuser beim Hinauswahlrechner oder als Benutzer mit einer entsprechenden Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Bearbeiten Sie die `/etc/ppp/peers/`*peer-name*-Datei des Peers, der aufgerufen werden soll.**

3 **Fügen Sie `-v` als Argument dem `chat`-Befehl hinzu, der in der `connect`-Option angegeben ist.**

```
connect "/usr/bin/chat -v -f /etc/ppp/chat-script-name"
```

4 Zeigen Sie Chat-Skript-Fehler in der Datei `/etc/ppp/connect-errors` an.

Es folgt der häufigste Fehler, der in Verbindung mit `chat` auftritt:

```
Oct 31 08:57:13 deino chat[107294]: [ID 702911 local2.info] expect (CONNECT)
Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] alarm
Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] Failed
```

Im Beispiel wird die Zeitüberschreitung während des Wartens auf eine `(CONNECT)`-Zeichenfolge dargestellt. Wenn `chat` fehlschlägt, erhalten Sie die folgende Meldung von `pppd` :

```
Connect script failed
```

Allgemeine Chat-Skript-Probleme

Chat-Skripten für Wählverbindungen sind fehleranfällig. In der folgenden Tabelle werden allgemeine Chat-Skript-Fehler sowie Empfehlungen zur Beseitigung der Fehler aufgeführt. Informationen zur Verfahrensweise finden Sie unter „So rufen Sie Informationen zur Fehlersuche für Chat-Skripten ab“ auf Seite 516.

TABELLE 21–5 Allgemeine Chat-Skript-Probleme

Symptom	Problem	Lösung
Die `pppd debug`-Ausgabe enthält die Meldung `Connect script failed`.	Mit Ihrem Chat-Skript werden ein Benutzername und ein Passwort bereitgestellt. `ogin:` *user-name* `ssword:` *password* Der Peer, der verbunden werden soll, fragt diese Informationen jedoch nicht ab.	1. Entfernen Sie den Benutzernamen und das Passwort aus dem Chat-Skript. 2. Versuchen Sie erneut, den Peer aufzurufen. 3. Wenn die Meldung weiterhin angezeigt wird, wenden Sie sich an den ISP. Erfragen Sie beim ISP die richtige Anmeldesequenz.

Das `/usr/bin/chat -v`-Protokoll enthält die Meldung `"expect (login:)" alarm read timed out`.	Mit Ihrem Chat-Skript werden ein Benutzername und ein Passwort bereitgestellt.
	`ogin: pppuser`
	`ssword: \q\U`
	Der Peer, der verbunden werden soll, fragt diese Informationen jedoch nicht ab.
		1. Entfernen Sie den Benutzernamen und das Passwort aus dem Chat-Skript.
		2. Versuchen Sie erneut, den Peer aufzurufen.
		3. Wenn die Meldung weiterhin angezeigt wird, wenden Sie sich an den ISP. Erfragen Sie beim ISP die richtige Anmeldesequenz.

TABELLE 21–5 Allgemeine Chat-Skript-Probleme *(Fortsetzung)*

Symptom	Problem	Lösung
Die `pppd debug`-Ausgabe enthält die Meldung `possibly looped-back .`	Der lokale Rechner oder sein Peer hängt an der Befehlszeile, und PPP wird nicht ausgeführt. Im Chat-Skript befinden sich ein falsch konfigurierter Anmeldename und ein falsch konfiguriertes Passwort.	1. Entfernen Sie den Benutzernamen und das Passwort aus dem Chat-Skript. 2. Versuchen Sie erneut, den Peer aufzurufen. 3. Wenn die Meldung weiterhin angezeigt wird, wenden Sie sich an den ISP. Erfragen Sie die richtige Anmeldesequenz.
Die `pppd debug`-Ausgabe zeigt, dass LCP aktiviert ist, aber die Verbindung kurze Zeit später beendet wird.	Das Passwort im Chat-Skript ist möglicherweise falsch.	1. Stellen Sie sicher, dass dem lokalen Rechner das richtige Passwort zur Verfügung steht. 2. Prüfen Sie das Passwort im Chat-Skript. Korrigieren Sie das Passwort, wenn es sich um ein falsches Passwort handelt. 3. Versuchen Sie erneut, den Peer aufzurufen. 4. Wenn die Meldung weiterhin angezeigt wird, wenden Sie sich an den ISP. Erfragen Sie beim ISP die richtige Anmeldesequenz.

Der Text vom Peer beginnt mit einer Tilde (~).	Mit Ihrem Chat-Skript werden ein Benutzername und ein Passwort bereitgestellt.
	`ogin: pppuser`
	`ssword: \q\U`
	Der Peer, der verbunden werden soll, fragt diese Informationen jedoch nicht ab.
		1. Entfernen Sie den Benutzernamen und das Passwort aus dem Chat-Skript.
		2. Versuchen Sie erneut, den Peer aufzurufen.
		3. Wenn die Meldung weiterhin angezeigt wird, wenden Sie sich an den ISP. Erfragen Sie die richtige Anmeldesequenz.

Das Modem hängt.	Ihr Chat-Skript enthält die folgende Zeile, durch die der lokale Rechner gezwungen wird, auf die `CONNECT`-Meldung vom Peer zu warten: `CONNECT ”`	Verwenden Sie die folgende Zeile, wenn das Chat-Skript auf die CONNECT-Meldung vom Peer warten soll: `CONNECT \c` Beenden Sie das Chat-Skript mit ~ `\c`.
Die `pppd debug`-Ausgabe enthält die Meldung `LCP: timeout sending Config-Requests`.	Ihr Chat-Skript enthält die folgende Zeile, durch die der lokale Rechner gezwungen wird, auf die `CONNECT`-Meldung vom Peer zu warten: `CONNECT ”`	Verwenden Sie die folgende Zeile, wenn das Chat-Skript auf die CONNECT-Meldung vom Peer warten soll: `CONNECT \c` Beenden Sie das Chat-Skript mit ~ `\c`.

TABELLE 21–5 Allgemeine Chat-Skript-Probleme *(Fortsetzung)*

Symptom	Problem	Lösung
Die `pppd debug`-Ausgabe enthält die Meldung `Serial link is not 8-bit clean`.	Ihr Chat-Skript enthält die folgende Zeile, durch die der lokale Rechner gezwungen wird, auf die `CONNECT`-Meldung vom Peer zu warten: `CONNECT ”`	Verwenden Sie die folgende Zeile, wenn das Chat-Skript auf die CONNECT-Meldung vom Peer warten soll: `CONNECT \c` Beenden Sie das Chat-Skript mit ~ `\c`.
Die `pppd debug`-Ausgabe enthält die Meldung `Loopback detected`.	Ihr Chat-Skript enthält die folgende Zeile, durch die der lokale Rechner gezwungen wird, auf die `CONNECT`-Meldung vom Peer zu warten: `CONNECT ”`	Verwenden Sie die folgende Zeile, wenn das Chat-Skript auf die CONNECT-Meldung vom Peer warten soll: `CONNECT \c` Beenden Sie das Chat-Skript mit ~ `\c`.
Die `pppd debug`-Ausgabe enthält die Meldung `SIGHUP`.	Ihr Chat-Skript enthält die folgende Zeile, durch die der lokale Rechner gezwungen wird, auf die `CONNECT`-Meldung vom Peer zu warten: `CONNECT ”`	Verwenden Sie die folgende Zeile, wenn das Chat-Skript auf die CONNECT-Meldung vom Peer warten soll: `CONNECT \c` Beenden Sie das Chat-Skript mit ~ `\c`.

▼ So diagnostizieren und beheben Sie Probleme im Zusammenhang mit der Übertragungsrate einer seriellen Verbindung

Einwahlserver können von Problemen betroffen sein, die auf Übertragungsraten zurückzuführen sind, die miteinander in Konflikt stehen. Anhand des folgenden Verfahrens können Sie die Ursache des Verbindungsproblems isolieren, das auf Übertragungsraten einer seriellen Verbindung zurückzuführen ist, die miteinander in Konflikt stehen.

Durch folgendes Verhalten werden Probleme im Zusammenhang mit Übertragungsraten verursacht:

- Sie haben PPP über ein Programm wie `/bin/login` aufgerufen und die Übertragungsrate der Verbindung festgelegt.
- Sie haben PPP über `mgetty` gestartet und versehentlich die Bitrate angegeben.

pppd ändert die ursprünglich für die Verbindung festgelegte Übertragungsrate in die Rate, die von `/bin/login` oder `mgetty` festgelegt wurde. Dies führt zum Fehlschlagen der Verbindung.

1. **Melden Sie sich beim Einwahlserver an. Stellen Sie sicher, dass die Fehlersuche deaktiviert ist, und rufen Sie den Peer auf.**

   Informationen zur Vorgehensweise finden Sie unter „So aktivieren Sie die PPP-Fehlersuche“ auf Seite 508.

2. **Zeigen Sie das resultierende `/var/log/pppdebug` -Protokoll an.**

   Prüfen Sie, ob in der Ausgabe die folgende Meldung enthalten ist:

   ```
   LCP too many configure requests
   ```

   Diese Meldung zeigt an, dass die Übertragungsraten der seriellen Verbindungen, die für PPP konfiguriert wurden, möglicherweise miteinander in Konflikt stehen.

3. **Prüfen Sie, ob PPP durch ein Programm wie `/bin/login` aufgerufen wird und die Übertragungsrate der Verbindung festgelegt wurde.**

   In diesem Fall ändert `pppd` die ursprünglich konfigurierte Übertragungsrate in die Rate, die in `/bin/login` angegeben ist.

4. **Prüfen Sie, ob ein Benutzer PPP mithilfe des Befehls `mgetty` gestartet und versehentlich eine Bitrate angegeben hat.**

   Daraus resultiert ebenfalls ein Konflikt der Übertragungsraten von seriellen Verbindungen.

5. **Beheben Sie das Problem wie folgt:**

   a. **Sperren Sie die DTE-Rate des Modems.**

   b. **Verwenden Sie nicht autobaud.**

   c. **Ändern Sie nach der Konfiguration nicht die Übertragungsrate der Verbindung.**

▼ So rufen Sie Diagnoseinformationen für PPPoE ab

Sie können PPP und standardmäßige UNIX-Dienstprogramme verwenden, um Probleme mit PPPoE zu lokalisieren. Wenn Sie vermuten, dass PPPoE die Ursache eines Verbindungsproblems ist, verwenden Sie die folgenden Diagnosetools, um Informationen zur Fehlerbehebung abzurufen.

1. **Melden Sie sich als Superuser beim Rechner an, auf dem der PPPoE-Tunnel ausgeführt wird, d. h. entweder beim PPPoE-Client oder beim PPPoE-Zugangsserver.**

2. **Aktivieren Sie die Fehlersuche. Informationen hierzu finden Sie unter „So aktivieren Sie die PPP-Fehlersuche“ auf Seite 508.**

3 Zeigen Sie den Inhalt der Protokolldatei `/var/log/pppdebug` an.

Im folgenden Beispiel wird ein Teil einer Protokolldatei dargestellt, die für eine Verbindung mit einem PPPoE-Tunnel erstellt wurde.

```
Sep  6 16:28:45 enyo pppd[100563]: [ID 702911 daemon.info] Plugin
  pppoe.so loaded.
Sep  6 16:28:45 enyo pppd[100563]: [ID 860527 daemon.notice] pppd
  2.4.0b1 (Sun Microsystems, Inc.,
Sep  5 2001 10:42:05) started by troot, uid 0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] connect option:
   '/usr/lib/inet/pppoec
-v hme0' started (pid 100564)
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Serial connection established.
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Using interface sppp0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.notice] Connect: sppp0
   <--> /dev/sppptun
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/pap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/chap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] sent
  [LCP ConfReq id=0xef <mru 1492>
asyncmap 0x0 <magic 0x77d3e953><pcomp><acomp>
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] rcvd
  [LCP ConfReq id=0x2a <mru 1402>
asyncmap 0x0 <magic 0x9985f048><pcomp><acomp
```

Wenn Sie das Problem nicht mithilfe der Fehlersuchausgabe isolieren können, fahren Sie mit diesem Verfahren fort.

4 Rufen Sie Diagnosemeldungen von PPPoE ab.

```
# pppd connect "/usr/lib/inet/pppoec -v interface-name"
```

`pppoec` sendet Diagnoseinformationen an `stderr` . Wenn Sie `pppd` im Vordergrund ausführen, wird die Ausgabe auf dem Bildschirm angezeigt. Wenn `pppd` im Hintergrund ausgeführt wird, wird die Ausgabe an `/etc/ppp/connect-errors` gesendet.

Im folgenden Beispiel werden die Meldungen dargestellt, die während der Aushandlung des PPPoE-Tunnels generiert werden.

```
Connect option: '/usr/lib/inet/pppoec -v hme0' started (pid 100564)
/usr/lib/inet/pppoec: PPPoE Event Open (1) in state Dead (0): action SendPADI (2)
/usr/lib/inet/pppoec: Sending PADI to ff:ff:ff:ff:ff:ff: 18 bytes
/usr/lib/inet/pppoec: PPPoE State change Dead (0) -> InitSent (1)
/usr/lib/inet/pppoec: Received Active Discovery Offer from 8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADO+ (5) in state InitSent (1): action SendPADR+ (5)
/usr/lib/inet/pppoec: Sending PADR to 8:0:20:cd:c1:2: 22 bytes
/usr/lib/inet/pppoec: PPPoE State change InitSent (1) -> ReqSent (3)
/usr/lib/inet/pppoec: Received Active Discovery Session-confirmation from
   8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADS (7) in state ReqSent (3): action Open (7)
/usr/lib/inet/pppoec: Connection open; session 0002 on hme0:pppoe
/usr/lib/inet/pppoec: PPPoE State change ReqSent (3) -> Convers (4)
/usr/lib/inet/pppoec: connected
```

Wenn Sie das Problem nicht mithilfe der Diagnosemeldungen isolieren können, fahren Sie mit diesem Verfahren fort.

5 Führen Sie snoop aus. Anschließend speichern Sie die Ablaufverfolgung in einer Datei.

Informationen zu snoop finden Sie auf der Manpage snoop(1M).

```
# snoop -o pppoe-trace-file
```

6 Zeigen Sie die snoop-Ablaufverfolgungsdatei an.

```
# snoop -i pppoe-trace-file -v pppoe

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 6:35:2.77
ETHER: Packet size = 32 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:78:f3:7c, Sun
ETHER: Ethertype = 8863 (PPPoE Discovery)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 9 (Active Discovery Initiation)
PPPoE: Session Id = 0
PPPoE: Length = 12 bytes
PPPoE:
PPPoE: ----- Service-Name -----
PPPoE: Tag Type = 257
PPPoE: Tag Length = 0 bytes
PPPoE:
PPPoE: ----- Host-Uniq -----
PPPoE: Tag Type = 259
PPPoE: Tag Length = 4 bytes
PPPoE: Data = Ox00000002
PPPoE:
.
.
.
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 5 arrived at 6:35:2.87
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:78:f3:7c, Sun)
ETHER: Source      = 0:2:fd:39:7f:7,
ETHER: Ethertype = 8864 (PPPoE Session)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 0 (PPPoE Session)
PPPoE: Session Id = 24383
PPPoE: Length = 20 bytes
PPPoE:
PPP: ----- Point-to-Point Protocol -----
```

```
PPP:
PPP-LCP: ----- Link Control Protocol -----
PPP-LCP:
PPP-LCP: Code = 1 (Configure Request)
PPP-LCP: Identifier = 80
PPP-LCP: Length = 18
```

Beheben von Standleitungsproblemen

Das häufigste Standleitungsproblem ist unzureichende Leistung. In den meisten Fällen müssen Sie sich an die Telefongesellschaft wenden, um das Problem zu beheben.

TABELLE 21–6 Allgemeine Standleitungsprobleme

Symptom	Problem	Lösung
Die Verbindung wird nicht gestartet.	CSU BPVs (CSU Bipolar Violations) können die Ursache sein. Ein Ende der Verbindung ist für AMI-Leitungen konfiguriert. Das andere Ende ist für ESF B8Zs (Bit–8 Zero substitute) konfiguriert.	Wenn Ihr Unternehmen in den USA oder Kanada angesiedelt ist, können Sie dieses Problem direkt über das Menü des CSU/DSU beheben. Informieren Sie sich in der Dokumentation des CSU/DSU-Herstellers. In anderen Ländern ist es möglicherweise die Aufgabe des Providers, CSU BPVs zu beheben.
Die Verbindung ist leistungsschwach.	In der `pppd debug`-Ausgabe werden CRC-Fehler aufgeführt, die auftreten, wenn die Verbindung durch anhaltenden Datenverkehr gekennzeichnet ist. Ihre Leitung kann von einem Taktproblem betroffen sein, das auf falsche eine Konfiguration zwischen der Telefongesellschaft und Ihrem Netzwerk zurückzuführen ist.	Setzen Sie sich mit der Telefongesellschaft in Verbindung, um sicherzustellen, dass "Loop Clocking" (Schleifentaktung) verwendet wird. Bei manchen unstrukturierten Standleitungen müssen Sie möglicherweise die Taktung unterstützen. Benutzer in Nordamerika sollten Loop Clocking verwenden.

Diagnostizieren und Beheben von Authentifizierungsproblemen

In der folgenden Tabelle werden Lösungen für allgemeine Authentifizierungsprobleme aufgeführt.

TABELLE 21–7 Allgemeine Authentifizierungsprobleme

Symptom	Problem	Lösung
Die `pppd debug`-Ausgabe zeigt die Meldung `Peer is not authorized to use remote address` *address*.	Sie verwenden die PAP-Authentifizierung. Die IP-Adresse für den Remote-Peer ist nicht in der `/etc/ppp/pap-secrets`-Datei enthalten.	Fügen Sie eine Sternchen (*) hinter dem Eintrag für den Peer in die `/etc/ppp/pap-secrets` -Datei ein.
Die `pppd debug`-Ausgabe zeigt, dass LCP gestartet, aber kurz danach beendet wird.	Das Passwort in der Datenbank für das betreffende Sicherheitsprotokoll ist möglicherweise falsch.	Prüfen Sie das Passwort des Peers in der `/etc/ppp/pap-secrets`- oder `/etc/ppp/chap-secrets`-Datei.

◆ ◆ ◆ KAPITEL 22

Solaris PPP 4.0 (Referenz)

In diesem Kapitel sind ausführliche konzeptionelle Informationen zu Solaris PPP 4.0 enthalten. Folgende Themen werden behandelt:

- „Verwenden von PPP-Optionen in Dateien und in der Befehlszeile“ auf Seite 525
- „Konfigurieren von benutzerspezifischen Optionen“ auf Seite 534
- „Angeben von Informationen für die Kommunikation mit dem Einwahlserver“ auf Seite 535
- „Konfigurieren der Modemgeschwindigkeit für eine Wählverbindung“ auf Seite 538
- „Definieren der Kommunikation über die Einwahlverbindung“ auf Seite 538
- „Authentifizieren von Anrufern“ auf Seite 549
- „Erstellen eines IP-Adressierungsschemas für Anrufer“ auf Seite 556
- „Erstellen von PPPoE-Tunneln für DSL-Unterstützung“ auf Seite 558

Verwenden von PPP-Optionen in Dateien und in der Befehlszeile

Solaris PPP 4.0 bietet zahlreiche Optionen, die Sie verwenden können, um Ihre PPP-Konfiguration zu definieren. Verwenden Sie diese Optionen in den PPP-Konfigurationsdateien oder in der Befehlszeile. Sie haben auch die Möglichkeit, die Dateien und Befehlszeilenoptionen zu kombinieren. Dieser Abschnitt enthält ausführliche Informationen zur Verwendung der PPP-Optionen in Konfigurationsdateien und als Argumente für PPP-Befehle.

Wo PPP-Optionen definiert werden können

Bei der Konfiguration von Solaris PPP 4.0 haben Sie viele Möglichkeiten. Sie können PPP-Optionen an folgenden Stellen definieren:

- PPP-Konfigurationsdateien
- PPP-Befehle, die in der Befehlszeile ausgegeben werden

- Kombination der beiden obigen Möglichkeiten

In der folgenden Tabelle werden die PPP-Konfigurationsdateien und -Befehle aufgeführt.

TABELLE 22–1 Übersicht der PPP-Konfigurationsdateien und -Befehle

Datei oder Befehl	Definition	Weitere Informationen
`/etc/ppp/options`	Eine Datei, in der die Eigenschaften enthalten sind, die standardmäßig für alle PPP-Verbindungen des Systems gelten. Beispielsweise kann ein Rechner Peers dazu auffordern, sich zu authentifizieren. Wenn diese Datei nicht vorhanden ist, wird Benutzern, die nicht als Root-Benutzer angemeldet sind, untersagt, PPP zu verwenden.	„`/etc/ppp/options`-Konfigurationsdatei“ auf Seite 530
`/etc/ppp/options.`*ttyname*	Eine Datei zur Beschreibung aller Eigenschaften der Kommunikation über den seriellen Port *ttyname*	„`/etc/ppp/options.`*ttyname*-Konfigurationsdatei“ auf Seite 531
`/etc/ppp/peers`	Ein Verzeichnis, in dem Informationen zu Peers vorhanden sind, mit denen ein Hinauswahlrechner verbunden wird. Die Dateien in diesem Verzeichnis werden zusammen mit der `call`-Option des `pppd`-Befehls verwendet.	„Angeben von Informationen für die Kommunikation mit dem Einwahlserver“ auf Seite 535
`/etc/ppp/peers/`*peer-name*	Eine Datei, in der die Eigenschaften des Remote-Peers *peer-name* enthalten sind. Zu den typischen Eigenschaften zählen die Telefonnummer des Remote-Peers und das Chat-Skript zum Aushandeln der Verbindung mit dem Peer.	„`/etc/ppp/peers/` *peer-name*-Datei“ auf Seite 535
`/etc/ppp/pap-secrets`	Eine Datei, in der die benötigten Sicherheitsberechtigungsnachweise für die PAP-Authentifizierung (Password Authentication Protocol) enthalten sind.	„`/etc/ppp/pap-secrets`-Datei“ auf Seite 549
`/etc/ppp/chap-secrets`	Eine Datei, in der die benötigten Sicherheitsberechtigungsnachweise für die CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol) enthalten sind.	„`/etc/ppp/chap-secrets`-Datei“ auf Seite 553
`~/.ppprc`	Eine Datei im Home-Verzeichnis eines PPP-Benutzers, die meist zusammen mit Einwahlservern verwendet wird. Diese Datei enthält bestimmte Informationen zu den Konfigurationen der einzelnen Benutzer.	„Konfigurieren von `$HOME/.ppprc` auf einem Einwahlserver“ auf Seite 534
`pppd` *Optionen*	Befehl und Optionen zum Initiieren einer PPP-Verbindung und zum Beschreiben der zugehörigen Eigenschaften	„Wie PPP-Optionen verarbeitet werden“ auf Seite 527

Informationen zu den PPP-Dateien finden Sie auf der Manpage pppd(1M). pppd (1M) enthält zudem umfassende Beschreibungen aller Optionen, die für den pppd -Befehl zur Verfügung stehen. In /etc/ppp sind Beispielvorlagen für alle PPP-Konfigurationsdateien verfügbar.

Wie PPP-Optionen verarbeitet werden

1. Der pppd-Dämon analysiert Folgendes:

   Alle Solaris PPP 4.0-Vorgänge werden vom pppd-Dämon durchgeführt, der gestartet wird, wenn ein Benutzer den pppd-Befehl ausführt. Wenn ein Benutzer einen Remote-Peer aufruft, geschieht Folgendes:

   - /etc/ppp/options
   - $HOME/.ppprc
   - Dateien, die durch die Option file oder call in /etc/ppp/options und $HOME/.ppprc geöffnet werden
2. pppd fragt die Befehlszeile ab, um festzustellen, welches Gerät verwendet wird. Der Dämon prüft noch keine Optionen, die vorgefunden werden.
3. pppd versucht anhand der folgenden Kriterien zu ermitteln, welches serielle Gerät verwendet werden soll:
   - Wenn ein serielles Gerät in der Befehlszeile oder in einer zuvor verarbeiteten Konfigurationsdatei angegeben ist, verwendet pppd den Namen des betreffenden Geräts.
   - Wenn kein serielles Gerät angegeben ist, sucht pppd in der Befehlszeile nach der Option notty, pty oder socket. Wenn eine dieser Optionen angegeben wird, geht pppd davon aus, dass kein Gerätename vorhanden ist.
   - Wenn pppd jedoch feststellt, dass ein Standardeintrag an ein tty angefügt ist, wird der Name des tty verwendet.
   - Wenn pppd noch immer kein serielles Gerät finden kann, beendet pppd die Verbindung und gibt einen Fehler aus.
4. pppd prüft dann, ob die Datei /etc/ppp/options.*ttyname* vorhanden ist. Wenn die Datei gefunden wird, wird sie von pppd analysiert.
5. pppd verarbeitet alle Optionen, die in der Befehlszeile angegeben sind.
6. pppd handelt das LCP (Link Control Protocol) aus, das zum Einrichten der Verbindung dient.
7. (Optional) Wenn eine Authentifizierung erforderlich ist, liest pppd die /etc/ppp/pap-secrets- oder /etc/ppp/chap-secrets-Datei, um den anderen Peer zu authentifizieren.

Die Datei /etc/ppp/peers/*peer-name* wird gelesen, wenn der pppd-Dämon die Option call *peer-name* in der Befehlszeile oder in den anderen Konfigurationsdateien findet.

Funktionsweise der PPP-Konfigurationsdateiberechtigungen

Die Solaris PPP 4.0-Konfiguration schließt das Konzept der *Berechtigungen* ein. Berechtigungen dienen zur Bestimmung des Vorrangs von Konfigurationsoptionen, insbesondere dann, wenn dieselbe Option an mehreren Stellen aufgerufen wird. Eine Option, die von einer privilegierten Quelle aufgerufen wird, hat Vorrang vor derselben Option, die von einer nicht privilegierten Quelle aufgerufen wird.

Benutzerberechtigungen

Der einzige privilegierte Benutzer ist der Superuser (`Root`-Benutzer) mit der UID null. Sämtliche anderen Benutzer sind nicht privilegiert.

Dateiberechtigungen

Die folgenden Konfigurationsdateien sind privilegierte Dateien, unabhängig davon, wer der Eigentümer der Dateien ist:

- `/etc/ppp/options`
- `/etc/ppp/options.`*`ttyname`*
- `/etc/ppp/peers/`*`peer-name`*

Die Datei `$HOME/.ppprc` ist im Besitz des Benutzers. Optionen, die über `$HOME/.ppprc` und die Befehlszeile gelesen werden können, sind nur dann privilegiert, wenn der Benutzer, der `pppd` aufruft, als `root`-Benutzer angemeldet ist.

Argumente, die nach der `file`-Option folgen, sind privilegiert.

Auswirkungen der Optionsberechtigungen

Manche Optionen erfordern eine Berechtigung des aufrufenden Benutzers oder der aufrufenden Quelle. Optionen, die über die Befehlszeile aufgerufen werden, verfügen über die Berechtigungen des Benutzers, der den `pppd`-Befehl ausführt. Diese Optionen sind nicht privilegiert, es sei denn, der Benutzer, der `pppd` aufruft, ist der `root`-Benutzer.

Option	Status	Erklärung
`domain`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`linkname`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`noauth`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`nopam`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`pam`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.

Option	Status	Erklärung
`plugin`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`privgroup`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`allow-ip` *addresses*	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`name` *hostname*	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`plink`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`noplink`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`plumbed`	Privilegiert	Es sind Berechtigungen zur Verwendung erforderlich.
`proxyarp`	Wird privilegiert, wenn `noproxyarp` angegeben wurde.	Kann nicht durch einen nicht privilegierten Vorgang außer Kraft gesetzt werden.
`defaultroute`	Privilegiert, wenn `nodefaultroute` in einer privilegierten Datei oder von einem privilegierten Benutzer angegeben wird.	Kann nicht durch einen nicht privilegierten Benutzer außer Kraft gesetzt werden.
`disconnect`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Kann nicht durch einen nicht privilegierten Benutzer außer Kraft gesetzt werden.
`bsdcomp`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Ein nicht privilegierter Benutzer kann keine Codegröße angeben, die größer als die Codegröße ist, die von einem privilegierten Benutzer angegeben wurde.
`deflate`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Ein nicht privilegierter Benutzer kann keine Codegröße angeben, die größer als die Codegröße ist, die von einem privilegierten Benutzer angegeben wurde.
`connect`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Kann nicht durch einen nicht privilegierten Benutzer außer Kraft gesetzt werden.
`init`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Kann nicht durch einen nicht privilegierten Benutzer außer Kraft gesetzt werden.
`pty`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Kann nicht durch einen nicht privilegierten Benutzer außer Kraft gesetzt werden.
`welcome`	Privilegiert bei Angabe in einer privilegierten Datei oder durch einen privilegierten Benutzer.	Kann nicht durch einen nicht privilegierten Benutzer außer Kraft gesetzt werden.

Option	Status	Erklärung
ttyname	Privilegiert bei Angabe in einer privilegierten Datei.	Geöffnet mit Root-Berechtigungen, unabhängig davon, welcher Benutzer `pppd` aufruft.
	Nicht privilegiert bei Angabe in einer nicht privilegierten Datei.	Geöffnet mit den Berechtigungen des Benutzers, der `pppd` aufruft.

`/etc/ppp/options`-Konfigurationsdatei

Verwenden Sie die `/etc/ppp/options` -Datei, um globale Optionen für die gesamte PPP-Kommunikation auf dem lokalen Rechner zu definieren. `/etc/ppp/options` ist eine privilegierte Datei. `/etc/ppp/options` sollte im Besitz des Root-Benutzers sein, obwohl diese Regel nicht von `pppd` erzwungen wird. Optionen, die Sie in `/etc/ppp/options` definieren, haben Vorrang vor den Definitionen derselben Optionen in allen anderen Dateien und in der Befehlszeile.

Zu den typischen Optionen in `/etc/ppp/options`, die Sie verwenden können, zählen folgende:

- **`lock`** – aktiviert die UUCP-basierte Dateisperrung.
- **`noauth`** – zeigt an, dass der Rechner keine Anrufer bzw. aufrufenden Programme authentifiziert.

Hinweis – Die Solaris PPP 4.0-Software enthält standardmäßig keine `/etc/ppp/options`-Datei. `pppd` benötigt nicht die `/etc/ppp/options` -Datei, um zu funktionieren. Wenn ein Rechner nicht über die `/etc/ppp/options` -Datei verfügt, kann `pppd` nur vom Root-Benutzer auf dem Rechner ausgeführt werden.

Sie müssen `/etc/ppp/options` mithilfe eines Texteditors erstellen (siehe „So definieren Sie die Kommunikation über die serielle Verbindung“ auf Seite 460). Wenn ein Rechner keine globalen Optionen benötigt, erstellen Sie eine leere `/etc/ppp/options`-Datei. Dann können sowohl der `root`-Benutzer als auch der normale Benutzer `pppd` auf dem lokalen Rechner ausführen.

`/etc/ppp/options.tmpl`-Vorlage

Die Datei `/etc/ppp/options.tmpl` enthält hilfreiche Kommentare zur `/etc/ppp/options`-Datei sowie drei allgemeine Optionen für die globale `/etc/ppp/options`-Datei.

```
lock
nodefaultroute
noproxyarp
```

Option	Definition
`lock`	Aktiviert die UUCP-basierte Dateisperrung
`nodefaultroute`	Gibt an, dass keine Standardroute definiert ist
`noproxyarp`	Weist `proxyarp` ab

Um `/etc/ppp/options.tmpl` als globale Optionsdatei zu verwenden, benennen Sie `/etc/ppp/options.tmpl` in `/etc/ppp/options` um. Anschließend modifizieren Sie die Inhalte der Datei entsprechend den Anforderungen Ihres Standorts.

Beispiele für `/etc/ppp/options`-Dateien

Beispiele für die `/etc/ppp/options`-Datei finden Sie in folgenden Quellen:

- Informationen zu einem Hinauswahlrechner finden Sie unter „So definieren Sie die Kommunikation über die serielle Verbindung“ auf Seite 460.
- Informationen zu einem Einwahlserver finden Sie unter „So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)“ auf Seite 468.
- Informationen zur PAP-Unterstützung auf einem Einwahlserver finden Sie unter „So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)“ auf Seite 481.
- Informationen zur PAP-Unterstützung für einen Hinauswahlrechner finden Sie unter „So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)“ auf Seite 485.
- Informationen zur CHAP-Unterstützung für einen Einwahlserver finden Sie unter „So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Einwahlserver)“ auf Seite 490.

`/etc/ppp/options.` *ttyname*-Konfigurationsdatei

Sie können die Kommunikationseigenschaften der seriellen Leitung in der `/etc/ppp/options.`*ttyname*-Datei konfigurieren. `/etc/ppp/options.`*ttyname* ist eine privilegierte Datei, die von `pppd` gelesen wird, nachdem vorhandene `/etc/ppp/options`- und `$HOME/.pprc` -Dateien analysiert wurden. Andernfalls liest `pppd` `/etc/ppp/options.`*ttyname* nach der Analyse von `/etc/ppp/options`.

ttyname wird sowohl für Einwahlverbindungen als auch Standleitungsverbindungen verwendet. *ttyname* stellt einen bestimmten seriellen Port eines Rechners dar, beispielsweise `cua/a` oder `cua/b`, an den ein Modem oder ein ISDN-TA angeschlossen sein kann.

Wenn Sie die `/etc/ppp/options.`*ttyname*-Datei benennen, ersetzen Sie den Schrägstrich (/) im Gerätenamen durch einen Punkt (.). Beispielsweise sollte die `options`-Datei für das Gerät `cua/b` mit `/etc/ppp/options.cua.b` benannt werden.

Hinweis – Es ist keine `/etc/ppp/options.` *ttyname*-Datei erforderlich, damit Solaris PPP 4.0 richtig funktioniert. Ihr Server hat möglicherweise nur eine serielle Leitung für PPP. Außerdem benötigt der Server wenige Optionen. In diesem Fall können Sie die notwendigen Optionen in einer anderen Konfigurationsdatei oder in der Befehlszeile angeben.

Verwenden von `/etc/ppp/options.` *ttyname* auf einem Einwahlserver

Erstellen Sie für eine Einwahlverbindung eine `/etc/ppp/options.`*ttyname* -Datei für jeden seriellen Anschluss auf einem Einwahlserver mit angeschlossenem Modem. Folgende Optionen stehen zur Verfügung:

- Vom Einwahlserver benötigte IP-Adresse

  Setzen Sie diese Option, wenn für Anrufe, die am Port *ttyname* eingehen, eine bestimmte IP-Adresse benötigt wird. Die in Ihrem Adressraum vorhandene Anzahl von IP-Adressen, die für PPP im Verhältnis zur Anzahl der potenziellen Anrufer zur Verfügung stehen, kann begrenzt sein. In diesem Fall sollten Sie in Erwägung ziehen, jeder seriellen Schnittstelle, die für PPP auf dem Einwahlserver verwendet wird, eine IP-Adresse zuzuweisen. Dadurch wird für PPP eine dynamische Adressierung implementiert.

- `asyncmap` *map-value*

  Die Option `asyncmap` dient der Zuordnung von Steuerzeichen, die nicht vom Modem oder dem ISDN-TA über die serielle Verbindung empfangen werden können. Wenn die Option `xonxoff` verwendet wird, setzt `pppd` automatisch ein asyncmap von 0xa0000.

  map-value gibt in hexadezimalem Format die Steuerzeichen an, die problembehaftet sind.

- `init "chat -U -f /etc/ppp/mychat"`

  Mithilfe der `init`-Option wird dem Modem mitgeteilt, die Kommunikation über die serielle Verbindung mithilfe der Informationen im `chat -U`-Befehl zu initialisieren. Das Modem verwendet die Chat-Zeichenfolge in der Datei `/etc/ppp/mychat`.

- Sicherheitsparameter, die auf der Manpage `pppd`(1m) aufgeführt sind

Verwenden von `/etc/ppp/options.` *ttyname* auf einem Einwahlrechner

Bei einem Hinauswahlrechner können Sie eine `/etc/ppp/options.` *ttyname*-Datei für den seriellen Port konfigurieren, der mit dem Modem verbunden ist, oder auf die Verwendung von `/etc/ppp/options.`*ttyname* verzichten.

Hinweis – Es ist keine `/etc/ppp/options.` *ttyname*-Datei erforderlich, damit Solaris PPP 4.0 richtig funktioniert. Ein Hinauswahlrechner hat möglicherweise nur eine serielle Leitung für PPP. Außerdem benötigt der Hinauswahlrechner eventuell ein paar Optionen. Sie können die erforderlichen Optionen in einer anderen Konfigurationsdatei oder in der Befehlszeile angeben.

`options.ttya.tmpl`-Vorlagendatei

Die `/etc/ppp/options.ttya.tmpl`-Datei enthält hilfreiche Kommentare zur `/etc/ppp/options.`*tty-name*-Datei. Die Vorlage enthält drei allgemeine Optionen für die `/etc/ppp/options.` *tty-name*-Datei.

```
38400
asyncmap 0xa0000
:192.168.1.1
```

Option	Definition
`38400`	Verwenden Sie diese Baudrate für Port ttya.
`asyncmap 0xa0000`	Weisen Sie den asyncmap-Wert 0xa0000 zu, sodass der lokale Rechner mit fehlerbehafteten Peers kommunizieren kann.
`:192.168.1.1`	Weisen Sie die IP-Adresse 192.168.1.1 allen Peers zu, die sich über die Verbindung einwählen.

Um `/etc/ppp/options.ttya.tmpl` für Ihren Standort zu verwenden, benennen Sie `/etc/ppp/options.tmpl` in `/etc/ppp/options.` *ttya-name* um. Ersetzen Sie *ttya-name* durch den Namen des seriellen Ports, an den das Modem angeschlossen ist. Anschließend modifizieren Sie die Inhalte der Datei entsprechend den Anforderungen Ihres Standorts.

Beispiele für die `/etc/ppp/options.`*ttyname*-Dateien

Beispiele für die `/etc/ppp/options.`*ttyname*-Dateien finden Sie in den folgenden Quellen:

- Informationen zu einem Hinauswahlrechner finden Sie unter „So definieren Sie die Kommunikation über die serielle Verbindung“ auf Seite 460.
- Informationen zu einem Einwahlserver finden Sie unter „So definieren Sie die Kommunikation über die serielle Verbindung (Einwahlserver)“ auf Seite 468.

Konfigurieren von benutzerspezifischen Optionen

Dieser Abschnitt enthält ausführliche Informationen zum Einrichten von Benutzern auf dem Einwahlserver.

Konfigurieren von `$HOME/.ppprc` auf einem Einwahlserver

Die Datei `$HOME/.ppprc` ist für Benutzer bestimmt, die bevorzugte PPP-Optionen konfigurieren. Als Administrator können Sie für Benutzer auch `$HOME/.ppprc` konfigurieren.

Die Optionen in `$HOME/.ppprc` sind nur dann privilegiert, wenn der Benutzer, der die Datei aufruft, ein privilegierter Benutzer ist.

Wenn ein Benutzer den `pppd`-Befehl verwendet, um einen Aufruf zu initiieren, ist die `.ppprc`-Datei die zweite Datei, die vom `pppd`-Dämon geprüft wird.

Unter „Einrichten von Benutzern der Einwahlservers“ auf Seite 466 finden Sie Anweisungen zum Einrichten von `$HOME/ .ppprc` auf dem Einwahlserver.

Konfigurieren von `$HOME/.ppprc` auf einem Hinauswahlrechner

Die `$HOME/.ppprc`-Datei ist für eine fehlerfreie Funktionsweise von Solaris PPP 4.0 auf dem Hinauswahlrechner nicht erforderlich. `$HOME/.ppprc` ist auf dem Hinauswahlrechner außerdem nur unter besonderen Umständen erforderlich. Erstellen Sie eine oder mehrere `.ppprc`-Dateien, indem Sie wie folgt vorgehen:

- Gestatten Sie mehreren Benutzern mit verschiedenen Kommunikationsanforderungen, über denselben Rechner Remote-Peers aufzurufen. Dazu erstellen Sie `.ppprc`-Dateien in den jeweiligen Home-Verzeichnissen der Benutzer, die hinauswählen müssen.
- Geben Sie Optionen an, mit deren Hilfe Probleme überwacht werden, die Ihre Verbindung betreffen, beispielsweise Deaktivierung der Van Jacobson-Komprimierung. Informationen zur Fehlersuche bei Verbindungen finden Sie in *PPP Design, Implementation, and Debugging* von James Carlson und auf der Manpage `pppd(1M)`.

Da die `.ppprc`-Datei meist zum Konfigurieren eines Einwahlservers verwendet wird, sollten Sie sich unter „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466 über die Konfigurationsanweisungen für `.ppprc` informieren.

Angeben von Informationen für die Kommunikation mit dem Einwahlserver

Um mit einem Einwahlserver zu kommunizieren, müssen Sie Informationen über den Server sammeln. Anschließend bearbeiten Sie einige Dateien. Vor allem müssen Sie die Kommunikationsanforderungen aller Einwahlserver definieren, die vom Hinauswahlrechner angewählt werden müssen. Sie können die Optionen für einen Einwahlserver (z. B. eine ISP-Telefonnummer) in der `/etc/ppp/options.` *ttyname*-Datei angeben. Am besten jedoch ist es, Peer-Informationen in den `/etc/ppp/peers/`*peer-name*-Dateien zu definieren.

`/etc/ppp/peers/` *peer-name*-Datei

Hinweis – Die `/etc/ppp/peers/`*peer-name* -Datei ist nicht auf einem Hinauswahlrechner erforderlich, um Solaris PPP 4.0 richtig auszuführen.

Verwenden Sie die `/etc/ppp/peers/`*peer-name*-Datei, um Informationen zum Kommunizieren mit einem bestimmten Peer bereitzustellen. `/etc/ppp/peers/` *peer-name* ermöglicht normalen Benutzern, vorgewählte privilegierte Optionen aufzurufen, die nicht von Benutzern festgelegt werden dürfen.

Ein nicht privilegierter Benutzer kann beispielsweise nicht die Option `noauth` außer Kraft setzen, wenn `noauth` in der `/etc/ppp/peers/` *peer-name*-Datei angegeben ist. Es wird angenommen, der Benutzer beabsichtigt, eine Verbindung mit `peerB` einzurichten, der keine Authentifizierungs-Berechtigungsnachweise bereitstellt. Als Superuser können Sie eine `/etc/ppp/peers/peerB`-Datei bereitstellen, in der die Option `noauth` enthalten ist. `noauth` gibt an, dass der lokale Rechner keine Aufrufe von `peerB` authentifiziert.

Der `pppd`-Dämon liest `/etc/ppp/peers/` *peer-name*, wenn `pppd` die folgende Option vorfindet:

`call` *peer-name*

Sie können eine `/etc/ppp/peers/`*peer-name* -Datei für jeden Ziel-Peer erstellen, mit dem der Hinauswahlrechner kommunizieren muss. Dieses Vorgehen ist besonders praktisch, wenn normalen Benutzern gestattet werden soll, ohne Root-Berechtigungen spezielle Hinauswahlverbindungen aufzurufen.

In `/etc/ppp/peers/`*peer-name* können Sie folgende Optionen angeben:

- `user` *user-name*

  Verwenden Sie *user-name* als Anmeldenamen des Hinauswahlrechners für den Einwahlserver, wenn Sie eine Authentifizierung mit PAP oder CHAP durchführen.

- `remotename` *peer-name*

Verwenden Sie *peer-name* als Namen des Einwahlrechners. `remotename` wird in Verbindung mit der PAP- oder CHAP-Authentifizierung verwendet, wenn die `/etc/ppp/pap-secrets`- oder `/etc/ppp/chap-secrets`-Dateien abgefragt werden.

- `connect "chat` *chat_script* `..."`

  Starten Sie die Kommunikation mit dem Einwahlserver, indem Sie die Anweisungen im Chat-Skript verwenden.

- `noauth`

  Authentifizieren Sie nicht den Peer *peer-name*, wenn Sie die Kommunikation initiieren.

- `noipdefault`

  Setzten Sie die anfängliche IP-Adresse, die zur Aushandlung mit dem Peer verwendet wird, auf 0.0.0.0. Sie können `noipdefault` zum Einrichten einer Verbindung mit den meisten ISPs verwenden, um die IPCP-Aushandlung zwischen den Peers zu vereinfachen.

- `defaultroute`

  Installieren Sie eine standardmäßige IPv4-Route, wenn die IP über die Verbindung eingerichtet ist.

Auf der Manpage pppd(1M) finden Sie weitere Optionen, die für einen bestimmten Ziel-Peer verwendet werden können.

`/etc/ppp/peers/myisp.tmpl`-Vorlagendatei

Die Datei `/etc/ppp/peers/myisp.tmpl` enthält hilfreiche Kommentare zur `/etc/ppp/peers/`*peer-name* -Datei. Die Vorlage endet mit allgemeinen Optionen, die Sie für eine `/etc/ppp/peers/`*peer-name*-Datei verwenden können:

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

Option	Definition
`connect "/usr/bin/chat -f /etc/ppp/myisp-chat"`	Ruft den Peer mithilfe des Chat-Skripts `/etc/ppp/myisp-chat` auf.
`user myname`	Verwenden Sie diesen Kontonamen für den lokalen Rechner. `myname` ist der Name für diesen Rechner, der in der `/etc/ppp/pap-secrets`-Datei des Peers angegeben ist.

Option	Definition
`remotename myisp`	Erkennt `myisp` als den Namen des Peers, der in der `/etc/ppp/pap-secrets`-Datei des lokalen Rechners angegeben ist.
`noauth`	Erfordert keinen Aufruf von Peers für die Bereitstellung von Authentifizierungs-Berechtigungsnachweisen.
`noipdefault`	Verwendet keine standardmäßige IP-Adresse für den lokalen Rechner.
`defaultroute`	Verwendet die standardmäßige Route, die dem lokalen Rechner zugewiesen ist.
`updetach`	Protokolliert Fehler in den PPP-Protokolldateien anstatt in der standardmäßigen Ausgabe.
`noccp`	Verwendet keine CCP-Komprimierung.

Um `/etc/ppp/peers/myisp.tmpl` an Ihrem Standort zu verwenden, benennen Sie `/etc/ppp/peers/myisp.tmpl` in `/etc/ppp/peers/`.*peer-name* um. Ersetzen Sie *peer-name* durch den Namen des Peers, der aufgerufen werden soll. Anschließend modifizieren Sie die Inhalte der Datei entsprechend den Anforderungen Ihres Standorts.

Beispiele für die `/etc/ppp/peers/`*peer-name*-Dateien

Beispiele für `/etc/ppp/peers/`*peer-name* -Dateien finden Sie in den folgenden Quellen:

- Informationen zu einem Hinauswahlrechner finden Sie unter „So definieren Sie die Verbindung mit einem bestimmten Peer“ auf Seite 462.
- Informationen zu einem lokalen Rechner an einer Standleitung finden Sie unter „So konfigurieren Sie einen Rechner an einer Standleitung“ auf Seite 474.
- Informationen zur Unterstützung der PAP-Authentifizierung für einen Hinauswahlrechner finden Sie unter „So fügen Sie PAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)“ auf Seite 485.
- Informationen zur Unterstützung der CHAP-Authentifizierung für einen Hinauswahlrechner finden Sie unter „So fügen Sie CHAP-Unterstützungsoptionen in die PPP-Konfigurationsdateien ein (Hinauswahlrechner)“ auf Seite 492.
- Informationen zur Unterstützung von PPPoE auf einem Clientsystem finden Sie unter „Einrichten des PPPoE-Clients“ auf Seite 496.

Konfigurieren der Modemgeschwindigkeit für eine Wählverbindung

Ein großes Problem bei der Konfiguration eines Modems ist die Festlegung der Geschwindigkeit, mit der ein Modem laufen soll. Die folgenden Richtlinien gelten für Modems, die in Verbindung mit Sun Microsystems-Computern verwendet werden:

- Ältere SPARC-Systeme – Entnehmen Sie die erforderlichen Informationen der begleitenden Hardwaredokumentation. Bei vielen SPARCstation-Rechnern darf die Modemgeschwindigkeit nicht über 38400 Bit/s liegen.
- UltraSPARC-Rechner – Setzen Sie die Modemgeschwindigkeit auf 115200 Bit/s. Dies empfiehlt sich für moderne Modems und ist schnell genug für eine Wählverbindung. Wenn Sie vorhaben, einen Zweikanal-ISDN-TA mit Komprimierung zu verwenden, müssen Sie die Modemgeschwindigkeit erhöhen. Der Grenzwert bei UltraSPARC liegt bei 460800 Bit/s im Fall einer asynchronen Verbindung.

Bei einem *Hinauswahlrechner* definieren Sie die Modemgeschwindigkeit in den PPP-Konfigurationsdateien (z. B. `/etc/ppp/peers/` *peer-name*), oder geben Sie die Geschwindigkeit als Option für `pppd` an.

Bei einem *Einwahlserver* legen Sie die Geschwindigkeit fest, indem Sie die `ttymon`-Funktion oder die Solaris Management Console verwenden. Informationen zur Vorgehensweise finden Sie unter „Konfigurieren von Geräten auf dem Einwahlserver“ auf Seite 464.

Definieren der Kommunikation über die Einwahlverbindung

Der Hinauswahlrechner und sein Remote-Peer kommunizieren über die PPP-Verbindung, indem Aushandlungen durchgeführt und verschiedene Anweisungen ausgetauscht werden. Wenn Sie einen Hinauswahlrechner konfigurieren, müssen Sie festlegen, welche Anweisungen vom lokalen Modem und vom Remote-Modem benötigt werden. Anschließend erstellen Sie eine Datei, in der die entsprechenden Anweisungen enthalten sind. Diese Datei wird als Chat-Skript bezeichnet. Dieser Abschnitt enthält Informationen zum Konfigurieren von Modems und zum Erstellen von Chat-Skripten.

Inhalt des Chat-Skripts

Jeder Remote-Peer, für den der Hinauswahlrechner eine Verbindung herstellen muss, erfordert möglicherweise ein eigenes Chat-Skript.

Hinweis – Chat-Skripten werden normalerweise nur für Wählverbindungen verwendet. Standleitungsverbindungen verwenden keine Chat-Skripten, es sei denn, die Verbindung enthält eine asynchrone Schnittstelle, für die eine Startkonfiguration erforderlich ist.

Der Inhalt des Chat-Skripts wird entsprechend den Anforderungen Ihres Modemmodells oder des ISDN-TA und des Remote-Peers festgelegt. Dieser Inhalt wird als Gruppe von expect-send-Zeichenfolgen angezeigt. Der Hinauswahlrechner und seine Remote-Peers tauschen die Zeichenfolgen während der Initiierung der Kommunikation aus.

Eine *expect*-Zeichenfolge enthält Zeichen, die der Hinauswahl-Hostrechner vom Remote-Peer erwartet, um mit der Kommunikation zu beginnen. Eine *send*-Zeichenfolge enthält Zeichen, die vom Hinauswahlrechner an den Remote-Peer gesendet werden, nachdem der Hinauswahlrechner die erwartete Zeichenfolge erhalten hat.

Das Chat-Skript enthält normalerweise folgende Informationen:

- Modembefehle, die oft als *AT-Befehle* bezeichnet werden und dem Modem ermöglichen, Daten über das Telefon zu übertragen
- Telefonnummer des Ziel-Peers

  Diese Telefonnummer kann die Nummer sein, die von Ihrem ISP, einem Einwahlserver am Firmenstandort oder einem einzelnen Rechner benötigt wird.
- Zeitüberschreitungswert (bei Bedarf)
- Anmeldesequenz, die vom Remote-Peer erwartet wird
- Anmeldesequenz, die vom Hinauswahlrechner gesendet wird

Beispiele für Chat-Skripten

In diesem Abschnitt werden Chat-Skripten aufgeführt, auf die Sie Bezug nehmen können, wenn Sie Ihre eigenen Chat-Skripten erstellen. Die Anleitung des Modemherstellers und die Informationen von Ihrem ISP und anderen Ziel-Hosts enthalten Chat-Anforderungen, die das Modem und Ihre Ziel-Peers betreffen. Außerdem sind Beispiele für Chat-Skripten auf zahlreichen PPP-Websites zu finden.

Grundlegendes Modem-Chat-Skript

Es folgt ein grundlegendes Chat-Skript, das Sie als Vorlage zum Erstellen von eigenen Chat-Skripten verwenden können.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
```

```
"" AT&F1M0&M5S2=255
SAY     "Calling myserver\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
ogin: pppuser
ssword: \q\U
% pppd
```

In der folgenden Tabelle wird der Inhalt des Chat-Skripts beschrieben.

Skriptinhalt	Erklärung
`ABORT BUSY`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`ABORT 'NO CARRIER'`	Bricht die Übertragung ab, wenn das Modem beim Wählen die Meldung `ABORT 'NO CARRIER'` sendet. Die Ursache für die Ausgabe dieser Meldung ist in der Regel ein Wählfehler oder ein Modemaushandlungsfehler.
`REPORT CONNECT`	Erfasst die `CONNECT`-Zeichenfolge, die vom Modem kommt. Gibt die Zeichenfolge aus.
`TIMEOUT 10`	Legt die anfängliche Zeitüberschreitung auf 10 Sekunden fest. Das Modem sollte unverzüglich antworten.
`"" AT&F1M0&M5S2=255`	`M0` – schaltet den Sprecher während des Verbindungsvorgangs ab. `&M5` – bewirkt, dass vom Modem eine Fehlerkontrolle verlangt wird. `S2=255` – deaktiviert die TIES "+++"-Unterbrechungssequenz.
`SAY "Calling myserver\n"`	Auf dem lokalen Rechner wird die Meldung `Calling myserver` angezeigt.
`TIMEOUT 60`	Setzt die Zeitüberschreitung auf 60 Sekunden zurück, um mehr Zeit für die Aushandlung der Verbindung zuzulassen.
`OK "ATDT1-123-555-1212"`	Wählt den Remote-Peer mithilfe der Telefonnummer 123-555-1212 an.
`ogin: pppuser`	Führt eine Anmeldung beim Peer durch UNIX-basierte Anmeldung aus. Stellt den Benutzernamen `pppuser` bereit.
`ssword: \q\U`	`\q` – es erfolgt keine Protokollierung, wenn die Fehlersuche mit der Option `-v` ausgeführt wird. `\U` – Fügt den Inhalt der nach `-U` folgenden Zeichenfolge an der betreffenden Stelle entsprechend der Angabe in der Befehlszeile ein. Normalerweise ist in der Zeichenfolge das Passwort enthalten.
`% pppd`	Wartet auf die %-Shell-Eingabeaufforderung und führt den `pppd`-Befehl aus.

/etc/ppp/myisp-chat.tmpl-Chat-Skript-Vorlage

In dieser Version ist die Vorlage /etc/ppp/myisp-chat.tmpl enthalten, die Sie für Ihre Verwendungszwecke ändern können. /etc/ppp/myisp-chat.tmpl ähnelt dem grundlegenden Modem-Chat-Skript, mit der Ausnahme, das die Vorlage keine Anmeldesequenz enthält.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
""      "AT&F1"
OK      "AT&C1&D2"
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
```

Skriptinhalt	Erklärung
ABORT BUSY	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
ABORT 'NO CARRIER	Bricht die Übertragung ab, wenn das Modem beim Wählen die Meldung ABORT 'NO CARRIER' sendet. Die Ursache für die Ausgabe dieser Meldung ist in der Regel ein Wählfehler oder ein Modemaushandlungsfehler.
REPORT CONNECT	Erfasst die CONNECT-Zeichenfolge, die vom Modem kommt. Gibt die Zeichenfolge aus.
TIMEOUT 10	Legt die anfängliche Zeitüberschreitung auf 10 Sekunden fest. Das Modem sollte unverzüglich antworten.
"" "AT&F1"	Setzt das Modem auf die werkseitigen Standardeinstellungen zurück.
OK "AT&C1&D2"	Setzt den Modem zurück. Bei &C1 folgt dann das vom Modem kommende DCD dem Trägersignal. Wenn das Telefon aus irgendeinem Grund von der Remote-Seite aus aufgelegt wird, wird das DCD abgebrochen. Bei &D2 bewirkt die DTR-Übergang von high-to-low, dass das Modem "auflegt" oder frei wird.
SAY "Calling myisp\n"	Auf dem lokalen Rechner wird die Meldung "Calling myisp" angezeigt.
TIMEOUT 60	Setzt die Zeitüberschreitung auf 60 Sekunden zurück, um mehr Zeit für die Aushandlung der Verbindung zuzulassen.
OK "ATDT1-123-555-1212"	Ruft den Remote-Peer mithilfe der Telefonnummer 123-555-1212 auf.

Skriptinhalt	Erklärung
`CONNECT \c`	Wartet auf die `CONNECT`-Meldung, die vom Modem des anderen Peers gesendet wird.

Modem-Chat-Skript zum Anwählen eines ISP

Verwenden Sie das folgende Chat-Skript als Vorlage zum Aufrufen eines ISP durch einen Hinauswahlrechner mit einem U.S. Robotics Courier-Modem:

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

In der folgenden Tabelle wird der Inhalt des Chat-Skripts beschrieben.

Skriptinhalt	Erklärung
`ABORT BUSY`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`ABORT 'NO CARRIER'`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`REPORT CONNECT`	Erfasst die `CONNECT`-Zeichenfolge, die vom Modem kommt. Gibt die Zeichenfolge aus.
`TIMEOUT 10`	Legt die anfängliche Zeitüberschreitung auf 10 Sekunden fest. Das Modem sollte unverzüglich antworten.
`"" AT&F1M0M0M0M0&M5S2=255`	`M0` – schaltet den Sprecher während des Verbindungsvorgangs ab `&M5` – bewirkt, dass vom Modem eine Fehlerkontrolle verlangt wird. `S2=255` – deaktiviert die TIES "+++"-Unterbrechungssequenz.
`SAY "Calling myisp\n"`	Auf dem lokalen Rechner wird die Meldung `Calling myisp` angezeigt.
`TIMEOUT 60`	Setzt die Zeitüberschreitung auf 60 Sekunden zurück, um mehr Zeit für die Aushandlung der Verbindung zuzulassen.
`OK "ATDT1-123-555-1212"`	Ruft den Remote-Peer mithilfe der Telefonnummer 123-555-1212 auf.
`CONNECT \c`	Wartet auf die `CONNECT`-Meldung, die vom Modem des anderen Peers gesendet wird.

Skriptinhalt	Erklärung
`\r \d\c`	Wartet bis zum Ende der `CONNECT`-Meldung.
SAY "Connected; running PPP\n"	Auf dem lokalen Rechner wird die informative Meldung `Connected; running PPP` angezeigt.

Grundlegendes Chat-Skript, das für eine UNIX-basierte Anmeldung erweitert wurde

Das folgende Chat-Skript ist ein erweitertes grundlegendes Skript, das dazu dient, einen Remote-Solaris-Peer oder einen anderen UNIX-Peer aufzurufen. Dieses Chat-Skript wird unter „So erstellen Sie die Anweisungen zum Aufrufen eines Peers“ auf Seite 461 verwendet.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&F1&M5S2=255
TIMEOUT 60
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT 'ogin incorrect'
ssword: \qmypassword
"% " \c
SAY "Logged in.  Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

In der folgenden Tabelle werden die Parameter des Chat-Skripts erklärt.

Skriptinhalt	Erklärung
`TIMEOUT 10`	Legt die anfängliche Zeitüberschreitung auf 10 Sekunden fest. Das Modem sollte unverzüglich antworten.
`ABORT BUSY`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`ABORT 'NO CARRIER'`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`ABORT ERROR`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.

Skriptinhalt	Erklärung
`REPORT CONNECT`	Erfasst die `CONNECT`-Zeichenfolge, die vom Modem kommt. Gibt die Zeichenfolge aus.
`"" AT&F1&M5S2=255`	`&M5` – bewirkt, dass vom Modem eine Fehlerkontrolle verlangt wird. `S2=255` – deaktiviert die TIES "+++"-Unterbrechungssequenz.
`TIMEOUT 60`	Setzt die Zeitüberschreitung auf 60 Sekunden zurück, um mehr Zeit für die Aushandlung der Verbindung zuzulassen.
`OK ATDT1-123-555-1234`	Ruft den Remote-Peer mithilfe der Telefonnummer 123-555-1212 auf.
`CONNECT \c`	Wartet auf die `CONNECT`-Meldung, die vom Modem des anderen Peers gesendet wird.
`SAY "Connected; logging in.\n"`	Zur Angabe des Benutzerstatus wird die informative Meldung `Connected; logging in` angezeigt.
`TIMEOUT 5`	Ändert die Zeitüberschreitung zum schnellen Anzeigen der Eingabeaufforderung für die Anmeldung.
`ogin:--ogin: pppuser`	Wartet auf die Eingabeaufforderung für die Anmeldung. Wenn die Eingabeaufforderung nicht empfangen wird, wird ein RETURN-Befehl gesendet und gewartet. Anschließend wird der Benutzername `pppuser` an den Peer gesendet. Die anschließende Sequenz wird von den meisten ISPs als PAP-Anmeldung bezeichnet. Die PAP-Anmeldung steht jedoch in keinem Zusammenhang mit der PAP-Authentifizierung.
`TIMEOUT 20`	Setzt die Zeitüberschreitung auf 20 Sekunden, um eine langsame Passwort-Verifizierung zu erlauben.
`ssword: \qmysecrethere`	Wartet auf die Passwort-Eingabeaufforderung, die vom Peer gesendet wird. Sobald die Eingabeaufforderung empfangen wird, wird das Passwort `\qmysecrethere` gesendet. `\q` verhindert, dass das Passwort in die Systemprotokolldateien geschrieben wird.
`"% " \c`	Wartet auf eine Shell-Eingabeaufforderung, die vom Peer gesendet wird. Das Chat-Skript verwendet die C-Shell. Ändern Sie diesen Wert, wenn der Benutzer es vorzieht, sich mit einer anderen Shell anzumelden.
`SAY "Logged in. Starting PPP on peer system.\n"`	Die informative Meldung `Logged in. Starting PPP on peer system` wird angezeigt, um den Benutzerstatus anzugeben.
`ABORT 'not found'`	Bricht die Übertragung ab, wenn die Shell Fehler vorfindet.
`"" "exec pppd"`	Startet `pppd` auf dem Peer.
`~ \c`	Wartet auf den Start von PPP auf dem Peer.

Wenn PPP unmittelbar nach `CONNECT \c` gestartet wird, wird dies von ISPs oft als *PAP-Anmeldung* bezeichnet, obwohl die PAP-Anmeldung kein Teil der PAP-Authentifizierung ist.

Mit der Phrase `ogin:--ogin: pppuser` wird das Modem angewiesen, den Benutzernamen `pppuser` als Antwort auf die Anmelde-Eingabeaufforderung des Einwahlservers zu senden. `pppuser` ist der Name eines speziellen Benutzerkontos, der für den Remote-Benutzer `user1` auf dem Einwahlserver erstellt wurde. Anweisungen zum Erstellen von PPP-Benutzerkonten finden Sie unter „So konfigurieren Sie Benutzer des Einwahlservers“ auf Seite 466.

Chat-Skript für einen externen ISDN-TA

Das folgende Chat-Skript dient zum Aufrufen durch einen Hinauswahlrechner mit ZyXEL omni.net. ISDN-TA:

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255
OK ATDI18882638234
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

In der folgenden Tabelle werden die Parameter des Chat-Skripts erklärt.

Skriptinhalt	Erklärung
`SAY "Calling the peer"`	Zeigt diese Meldung auf dem Bildschirm des Hinauswahlrechners an.
`TIMEOUT 10`	Legt die anfängliche Zeitüberschreitung auf 10 Sekunden fest.
`ABORT BUSY`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`ABORT 'NO CARRIER'`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`ABORT ERROR`	Bricht die Übertragung ab, wenn das Modem diese Meldung vom anderen Peer empfängt.
`REPORT CONNECT`	Erfasst die `CONNECT`-Zeichenfolge, die vom Modem kommt. Gibt die Zeichenfolge aus.

Skriptinhalt	Erklärung
`"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255`	Die Buchstaben in dieser Zeile haben folgende Bedeutung: ■ `&F` – werkseite Standardeinstellung verwenden ■ `B40` – asynchrone PPP-Konvertierung ausführen ■ `S83.7=1` – Daten verwenden, die über das Sprachträgersignal gesendet werden ■ `&K44` – CCP-Komprimierung aktivieren ■ `&J3` – MP aktivieren ■ `X7` – Raten der DCE-Seite melden ■ `S61.3=1` – Paketfragmentierung verwenden ■ `S0=0` – keine automatische Antwort ■ `S2=255` – TIES-Escape-Sequenz deaktivieren
`OK ATDI18882638234`	Führt einen ISDN-Aufruf aus. Für einen Multilink wird der zweite Aufruf derselben Telefonnummer zugeordnet. Dies erfordern die meisten ISPs. Wenn der Remote-Peer eine andere zweite Telefonnummer anfordert, wird "+ *nnnn*." hinzugefügt. *nnnn* stellt die zweite Telefonnummer dar.
`CONNECT \c`	Wartet auf die `CONNECT`-Meldung, die vom Modem des anderen Peers gesendet wird
`\r \d\c`	Wartet bis zum Ende der `CONNECT`-Meldung.
`SAY "Connected; running PPP\n"`	Zeigt diese Meldung auf dem Bildschirm des Hinauswahlrechners an.

Beschreibungen der Optionen und andere ausführliche Informationen zu diesem Skript finden Sie auf der Manpage `chat(1M)`. Eine Erläuterung der expect-send-Zeichenfolgen finden Sie unter „Feld "Chapt Script" in `/etc/uucp/Systems`-Datei“ auf Seite 601.

Weitere Chat-Skript-Beispiele

Einige Websites bieten Beispiel-Chat-Skripten sowie Hilfe bei der Erstellung der Chat-Skripten. Entsprechende Informationen finden Sie beispielsweise unter http://ppp.samba.org/ppp/index.html .

Aufrufen des Chat-Skripts

Mithilfe der `connect`-Option können Sie Chat-Skripten aufrufen. Sie können `connect "chat ..."` in jeder PPP-Konfigurationsdatei oder in der Befehlszeile verwenden.

Chat-Skripten sind nicht ausführbar, aber das von `connect` aufgerufene Programm muss ausführbar sein. Sie können das Chat-Dienstprogramm als Programm verwenden, das von `connect` aufgerufen wird. Wenn Sie in diesem Fall das Chat-Skript mithilfe der Option `-f` in einer externen Datei speichern, ist Ihre Chat-Skript-Datei nicht ausführbar.

Das chat-Programm, das in chat(1m) beschrieben wird, dient zum Ausführen des Chat-Skripts. Der pppd -Dämon ruft das chat-Programm auf, wenn pppd die Option connect "chat ..." vorfindet.

Hinweis – Sie können jedes externe Programm (z. B. Perl oder Tcl) verwenden, um erweiterte Chat-Skripten zu erstellen. Das chat-Dienstprogramm wird bereitgestellt, um Ihnen die Arbeit zu erleichtern.

▼ So rufen Sie ein Chat-Skript auf (Aufgabe)

1. **Erstellen Sie das Chat-Skript als ASCII-Datei.**

2. **Rufen Sie das Chat-Skript in einer beliebigen PPP-Konfigurationsdatei auf, indem Sie die folgende Syntax verwenden:**

   ```
   connect 'chat  -f /etc/ppp/chatfile'
   ```

   Das -f-Flag zeigt an, dass ein Dateiname folgen soll. */etc/ppp/chatfile* stellt den Namen der Chat-Datei dar.

3. **Erteilen Sie dem Benutzer, der den pppd-Befehl ausführt, eine Leseberechtigung für die externe Chat-Datei.**

Achtung – Das Chat-Programm wird immer mit den Berechtigungen des Benutzers ausgeführt. Dies gilt auch dann, wenn die connect 'chat ...'-Option durch eine privilegierte Quelle aufgerufen wird. Aus diesem Grund muss eine separate Chat-Datei, die mithilfe der Option -f gelesen wird, vom aufrufenden Benutzer gelesen werden können. Diese Berechtigung kann ein Sicherheitsproblem sein, wenn im Chat-Skript Passwörter oder andere vertrauliche Informationen enthalten sind.

Beispiel 22–1 Einzeiliges Chat-Skript

Sie können den gesamten Chat-Skript-Dialog wie folgt in einer einzelnen Zeile unterbringen:

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

Dem kompletten Chat-Skript folgt das chat-Schlüsselwort. Das Skript endet mit "\c"'. Verwenden Sie diese Konstellation in jeder PPP-Konfigurationsdatei oder in der Befehlszeile als Argument für pppd .

Weitere Informationen:

Chat-Skript in einer externen Datei

Wenn das für einen bestimmten Peer benötigte Chat-Skript lang oder kompliziert ist, können Sie das Skript als separate Datei erstellen. Externe Chat-Dateien lassen sich unkompliziert verwalten und dokumentieren. Sie können Kommentare in die Chat-Datei einfügen. Vor den Kommentaren muss das Hash-Zeichen (#) stehen.

Unter „So erstellen Sie die Anweisungen zum Aufrufen eines Peers“ auf Seite 461 ist beschrieben, wie ein Chat-Skript verwendet wird, das in einer externen Datei enthalten ist.

Erstellen einer ausführbaren Chat-Datei

Sie können eine Chat-Datei erstellen, die ein ausführbares Skript ist, das automatisch ausgeführt wird, wenn eine Einwahlverbindung initiiert wird. Auf diese Weise können Sie während der Verbindungsinitiierung neben den Befehlen, die in einem herkömmlichen Chat-Skript enthalten sind, weitere Befehle wie beispielsweise `stty` für Paritätseinstellungen ausführen.

Dieses ausführbare Chat-Skript meldet sich bei einem älteren UNIX-System an, das 7 Bits mit gerader Parität verlangt. Das System wechselt dann auf 8 Bits ohne Parität, während PPP ausgeführt wird.

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

▼ So erstellen Sie ein ausführbares Chat-Programm

1. **Verwenden Sie einen Texteditor, um ein ausführbares Chat-Programm wie das im vorangegangenen Beispiel zu erstellen.**

2. **Stellen Sie sicher, dass das Programm ausführbar ist.**

   ```
   # chmod +x /etc/ppp/chatprogram
   ```

3. **Rufen Sie das Chat-Programm auf.**

   ```
   connect /etc/ppp/chatprogram
   ```

   Chat-Programme müssen sich nicht innerhalb des `/etc/ppp`-Dateisystems befinden. Sie können Chat-Programme an einer beliebigen Stelle speichern.

Authentifizieren von Anrufern

Dieser Abschnitt enthält Erklärungen zur Funktionsweise der PPP-Authentifizierungsprotokolle und der Datenbanken, die den Authentifizierungsprotokollen zugeordnet sind.

PAP (Password Authentication Protocol)

Die PAP-Authentifizierung ähnelt in ihrer Funktionsweise dem UNIX-Anmeldeprogramm, obwohl PAP den Benutzern keinen Shell-Zugriff erlaubt. PAP verwendet die PPP-Konfigurationsdateien und die PAP-Datenbank unter Zuhilfenahme der `/etc/ppp/pap-secrets`-Datei, um die Authentifizierung durchzuführen. Außerdem wird `/etc/ppp/pap-secrets` von PAP zum Definieren der PAP-Sicherheitsberechtigungsnachweise verwendet. Diese Berechtigungsnachweise umfassen einen Peer-Namen, einen "Benutzernamen" in PAP-Sprache und ein Passwort. Zu den PAP-Berechtigungsnachweisen zählen zudem relevante Informationen für jeden Anrufer, dem gestattet ist, eine Verbindung mit dem lokalen Rechner herzustellen. Die PAP-Benutzernamen und -Passwörter können mit den UNIX-Benutzernamen und -Passwörtern in der Passwortdatenbank übereinstimmen oder sich von diesen unterscheiden.

`/etc/ppp/pap-secrets`-Datei

Die PAP-Datenbank wird in der `/etc/ppp/pap-secrets` -Datei implementiert. In den `/etc/ppp/pap-secrets`-Dateien der Rechner, die sich an beiden Enden der PPP-Verbindung befinden, müssen richtig konfigurierte PAP-Berechtigungsnachweise enthalten sein, damit die Authentifizierung erfolgreich durchgeführt werden kann. Der Anrufer (Authentifizierungsempfänger) stellt Berechtigungsnachweise in den `user`- und `password`-Spalten der `/etc/ppp/pap-secrets`-Datei oder in der veralteten `+ua` -Datei bereit. Der Server (Authentifizierer) gleicht diese Berechtigungsnachweise mit den Informationen in `/etc/ppp/pap-secrets` ab, indem die `passwd`-UNIX-Datenbank oder die PAM-Funktion verwendet wird.

Die `/etc/ppp/pap-secrets`-Datei weist die folgende Syntax auf:

```
myclient ISP-server mypassword *
```

Die Parameter haben folgende Bedeutungen:

`myclient`	PAP-Benutzername des Anrufers. Dieser Name ist oft mit dem UNIX-Benutzernamen des Anrufers identisch, insbesondere dann, wenn der Einwahlserver die Anmeldeoption (`login`) von PAP verwendet.
`ISP-server`	Name des Remote-Rechners, bei dem es sich oft um einen Einwahlserver handelt
`mypassword`	PAP-Passwort des Anrufers

*	IP-Adresse des Anrufers. Verwenden Sie ein Sternchen (*), um eine IP-Adresse anzugeben.

Erstellen von PAP-Passwörtern

PAP-Passwörter werden *unverschlüsselt* über die Verbindung gesendet, d. h. in lesbarem ASCII-Format. Für den Anrufer (Authentifizierungsempfänger) muss das PAP-Passwort an folgenden Stellen unverschlüsselt gespeichert werden:

- In `/etc/ppp/pap-secrets`
- In einer anderen externen Datei
- In einer benannten Pipe durch die `pap-secrets` @-Funktion
- Als Option für `pppd` entweder in der Befehlszeile oder in einer PPP-Konfigurationsdatei
- Über die `+ua`-Datei

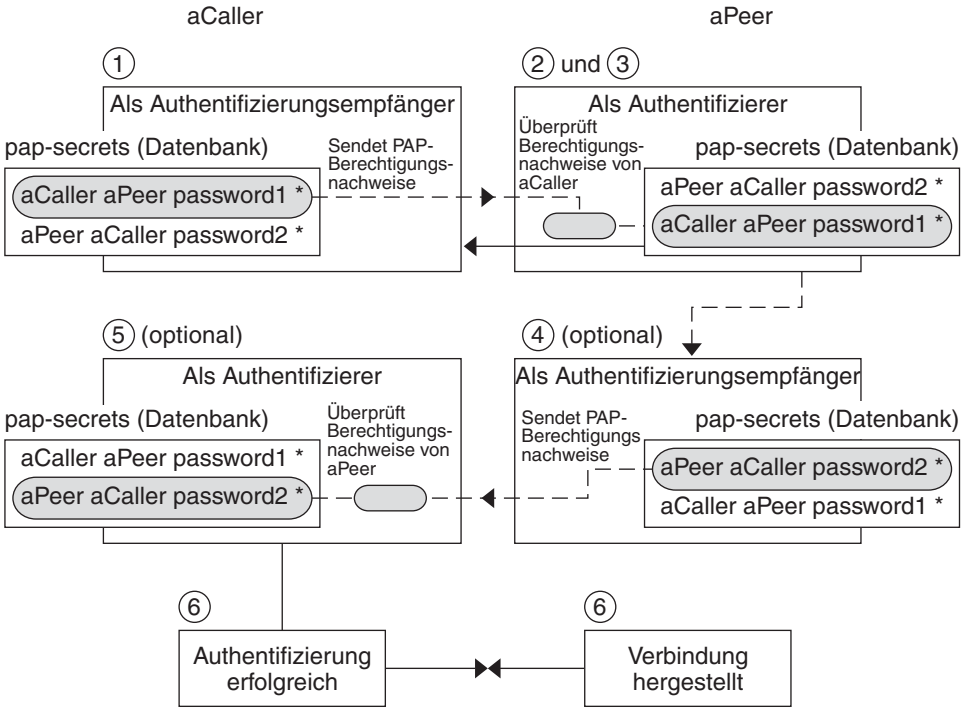
Auf dem Server (Authentifizierer) kann das PAP-Passwort wie folgt ausgeblendet werden:

- Angeben von `papcrypt` und Verwenden von Passwörtern, die durch `crypt`(3C) in der `pap-secrets`-Datei mit Hash-Codierung versehen werden
- Angeben der `login`-Option für `pppd` und Weglassen des Passworts in der `pap-secrets`-Datei durch Eintragen von doppelten Anführungszeichen ("") in die Passwort-Spalte In diesem Fall wird die Authentifizierung mithilfe der UNIX-Passwortdatenbank oder des `pam`(3pam)-Mechanismus durchgeführt.

Vorgänge während der PAP-Authentifizierung

Die PAP-Authentifizierung läuft wie folgt ab.

ABBILDUNG 22–1 PAP-Authentifizierungsprozess



1. Der Anrufer (Authentifizierungsempfänger) wählt den Remote-Peer (Authentifizierer) an und stellt seinen PAP-Benutzernamen und ein Passwort als Teil der Aushandlung der Verbindung bereit.
2. Der Peer prüft die Identität des Anrufers in der `/etc/ppp/pap-secrets` -Datei. Wenn der Peer die `login`-Option von PAP verwendet, verifiziert der Peer den Benutzernamen und das Passwort des Anrufers in seiner Passwortdatenbank.
3. Wenn die Authentifizierung erfolgreich ist, setzt der Peer die Aushandlung der Verbindung mit dem Anrufer fort. Schlägt die Authentifizierung fehl, wird die Verbindung abgebrochen.
4. (Optional) Wenn der Anrufer Antworten von Remote-Peers authentifiziert, muss der Remote-Peer seine eigenen PAP-Berechtigungsnachweise an den Anrufer senden. Dadurch wird der Remote-Peer zum Authentifizierungsempfänger und der Anrufer zum Authentifizierer.
5. (Optional) Der ursprüngliche Anrufer liest seine eigene `/etc/ppp/pap-secrets` , um die Identität des Remote-Peers zu verifizieren.

Hinweis – Wenn der ursprüngliche Anrufer Authentifizierungs-Berechtigungsnachweise vom Remote-Peer verlangt, werden Schritt 1 und 4 gleichzeitig ausgeführt.

Wenn der Peer authentifiziert ist, wird die Aushandlung fortgesetzt. Anderenfalls wird die Verbindung abgebrochen.

6. Die Aushandlung zwischen Anrufer und Peer wird fortgesetzt, bis die Verbindung hergestellt ist.

Verwenden der `login`-Option mit `/etc/ppp/pap-secrets`

Sie können die `login`-Option für die Authentifizierung von PAP-Berechtigungsnachweisen in jede PPP-Konfigurationsdatei einfügen. Wenn `login` beispielsweise in `/etc/ppp/options` angegeben wird, verifiziert `pppd`, dass die PAP-Berechtigungsnachweise des Anrufers in der Solaris-Passwortdatenbank enthalten sind. Im Folgenden wir das Format einer `/etc/ppp/pap-secrets`-Datei mit der `login`-Option dargestellt:

```
joe    *  ""  *
sally  *  ""  *
sue    *  ""  *
```

Die Parameter haben folgende Bedeutungen:

Anrufer	`joe`, `sally` und `sue` sind die Namen der autorisierten Anrufer.
Server	Sternchen (*), das anzeigt, dass ein Servername gültig ist. Die `name`-Option wird in den PPP-Konfigurationsdateien nicht benötigt.
Passwort	Doppelte Anführungszeichen, die anzeigen, dass ein Passwort gültig ist. Wenn in dieser Spalte ein Passwort enthalten ist, muss dass vom Peer gesendete Passwort sowohl mit dem PAP-Passwort als auch mit dem Passwort in der UNIX-Passwortdatenbank (`passwd`) übereinstimmen.
IP-Adressen	Sternchen (*), das anzeigt, dass eine beliebige IP-Adresse erlaubt ist.

CHAP (Challenge-Handshake Authentication Protocol)

Bei der CHAP-Authentifizierung wird das Konzept der *Aufforderung* und *Antwort* verwendet. Das bedeutet, dass der Peer (Authentifizierer) den Anrufer (Authentifizierungsempfänger) auffordert, seine Identität nachzuweisen. Die Aufforderung besteht aus einer Zufallszahl und

einer eindeutigen ID, die vom Authentifizierer generiert wird. Der Anrufer muss die ID, die Zufallszahl und seine CHAP-Sicherheitsberechtigungsnachweise verwenden, um die richtige Antwort (Handshake) an den Peer zu senden.

Zu den CHAP-Sicherheitsberechtigungsnachweisen gehören ein CHAP-Benutzername und ein "CHAP-Geheimnis". Das CHAP-Geheimnis ist eine beliebige Zeichenfolge, die sowohl dem Anrufer als auch dem Peer bekannt ist, bevor diese mit dem Aushandeln einer PPP-Verbindung beginnen. Die CHAP-Sicherheitsberechtigungsnachweise konfigurieren Sie in der CHAP-Datenbank, `/etc/ppp/chap-secrets`.

`/etc/ppp/chap-secrets`-Datei

Die CHAP-Datenbank ist in der `/etc/ppp/chap-secrets`-Datei implementiert. Die Rechner, die sich an beiden Enden der PPP-Verbindung befinden, müssen über die CHAP-Berechtigungsnachweise des jeweils anderen Rechners in den `/etc/ppp/chap-secrets` -Dateien verfügen, damit die Authentifizierung erfolgreich durchgeführt werden kann.

Hinweis – Anders als bei PAP muss das gemeinsame Geheimnis auf beiden Peers unverschlüsselt sein. Bei CHAP können die Optionen crypt, PAM oder PPP login nicht verwendet werden.

Die `/etc/ppp/chap-secrets` hat die folgende Syntax:

```
myclient myserver secret5748 *
```

Die Parameter haben folgende Bedeutungen:

`myclient` CLIENT-HOSTAP-Benutzername des Anrufers. Dieser Name kann mit dem UNIX-Benutzernamen des Anrufers übereinstimmen oder sich von diesem unterschieden.

`myserver` Name des Remote-Rechners, bei dem es sich oft um einen Einwahlserver handelt

`secret5748` CHAP-Geheimnis des Anrufers

Hinweis – Anders als bei PAP-Passwörtern werden CHAP-Geheimnisse nie über die Verbindung gesendet. Stattdessen werden CHAP-Geheimnisse verwendet, während die lokalen Rechner die Antwort berechnen.

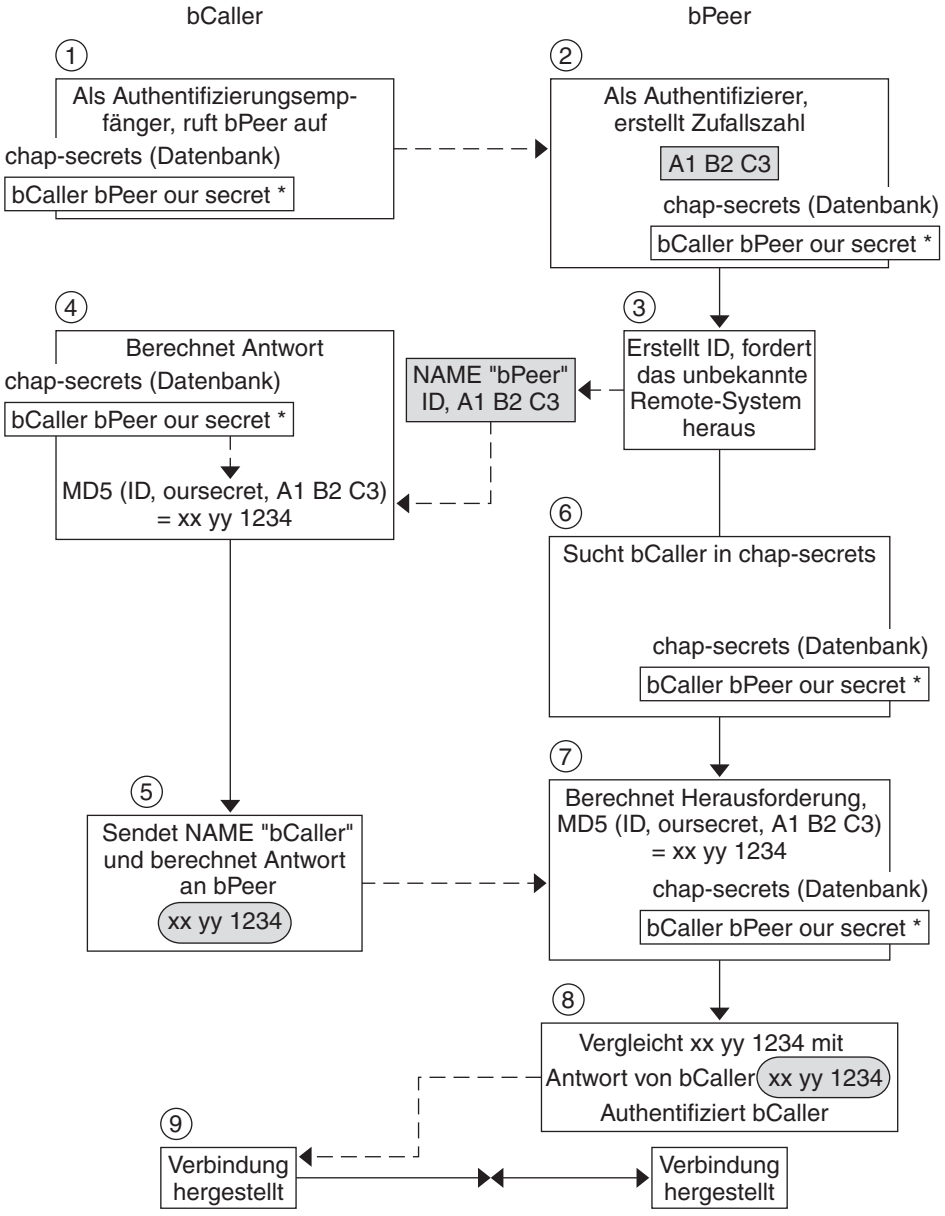
---

* IP-Adresse des Anrufers. Verwenden Sie ein Sternchen (*), um eine IP-Adresse anzugeben.

Vorgänge während der CLIENT-HOSTAP-Authentifizierung

Die CHAP-Authentifizierung läuft wie folgt ab.

ABBILDUNG 22–2 Ablauf der CHAP-Authentifizierung



1. Zwei Peers, die gerade im Begriff sind, die Kommunikation zu initiieren, vereinbaren ein Geheimnis, das während der Aushandlung einer PPP-Verbindung zur Authentifizierung verwendet werden soll.

2. Die Administratoren beider Rechner fügen das Geheimnis, die CHAP-Benutzernamen und andere CHAP-Berechtigungsnachweise in die `/etc/ppp/chap-secrets`-Datenbank der betreffenden Rechner ein.
3. Der Anrufer (Authentifizierungsempfänger) ruft den Remote-Peer (Authentifizierer) auf.
4. Der Authentifizierer genehmigt eine Zufallszahl und eine ID und sendet diese Daten als Aufforderung an den Authentifizierungsempfänger.
5. Der Authentifizierungsempfänger sucht in seiner `/etc/ppp/chap-secrets`-Datenbank nach dem Namen und dem Geheimnis des Peers.
6. Der Authentifizierungsempfänger berechnet eine Antwort, indem er den MD5-Berechnungsalgorithmus auf das Geheimnis und die Zufallszahl des Peers anwendet. Dann sendet der Authentifizierungsempfänger die Ergebnisse in Form einer Antwort an den Authentifizierer.
7. Der Authentifizierer sucht in seiner `/etc/ppp/chap-secrets`-Datenbank nach dem Namen und dem Geheimnis des Authentifizierungsempfängers.
8. Der Authentifizierer berechnet seine eigene Zahl, indem er MD5 auf die als Aufforderung generierte Zahl und das Geheimnis für den Authentifizierungsempfänger in `/etc/ppp/chap-secrets` anwendet.
9. Der Authentifizierer vergleicht seine Ergebnisse mit der Antwort des Anrufers. Wenn die beiden Zahlen übereinstimmen, ist der Anrufer erfolgreich vom Peer authentifiziert worden, und die Aushandlung der Verbindung wird fortgesetzt. Anderenfalls wird die Verbindung abgebrochen.

Erstellen eines IP-Adressierungsschemas für Anrufer

Sie können eine oder mehrere IP-Adressen für alle eingehenden Anrufe erstellen, anstatt jedem Remote-Benutzer eine eindeutige IP-Adresse zuzuweisen. Dedizierte IP-Adressen sind besonders wichtig, wenn die Anzahl der potenziellen Anrufer größer ist als die Anzahl der seriellen Ports und Modems auf dem Einwahlserver. Je nach den Anforderungen an Ihrem Standort können Sie eine Reihe verschiedener Szenarios implementieren. Außerdem schließen sich die Szenarios nicht gegenseitig aus.

Zuweisen von dynamischen IP-Adressen für Anrufer

Die dynamische Adressierung erfordert die Zuweisung der in `/etc/ppp/options.` *ttyname* definierten IP-Adresse für jeden Anrufer. Die dynamische Adressierung wird für jeweils einen seriellen Port durchgeführt. Wenn über eine serielle Verbindung ein Aufruf eingeht, empfängt der Anrufer die IP-Adresse, die in der `/etc/ppp/options.`*ttyname*-Datei für die serielle Schnittstelle des Aufrufs enthalten ist.

Ein Einwahlserver hat beispielsweise vier serielle Schnittstellen, die als Einwahlanschluss für eingehende Aufrufe dienen:

- Für den seriellen Port `term/a` erstellen Sie die Datei `/etc/ppp/options.term.a` mit dem folgenden Eintrag:

  ```
  :10.1.1.1
  ```
- Für den seriellen Port `term/b` erstellen Sie die Datei `/etc/ppp/options.term.b` mit dem folgenden Eintrag:

  ```
  :10.1.1.2
  ```
- Für den seriellen Port `term/c` erstellen Sie die Datei `/etc/ppp/options.term.c` mit dem folgenden Eintrag:

  ```
  :10.1.1.3
  ```
- Für den seriellen Port `term/d` erstellen Sie die Datei `/etc/ppp/options.term.d` mit dem folgenden Eintrag:

  ```
  :10.1.1.4
  ```

Unter Verwendung des zuvor erwähnten Adressierungsschemas erhält ein Aufruf, der an der seriellen Schnittstelle `/dev/term/c` eingeht, für die Dauer des Aufrufs die IP-Adresse 10.1.1.3. Nachdem der erste Anrufer aufgelegt hat, erhält eine späterer Aufruf, der über die serielle Schnittstelle `/dev/term/c` eingeht, ebenfalls die IP-Adresse 10.1.1.3.

Die dynamische Adressierung hat folgende Vorteile:

- Sie können die Nutzung des PPP-Netzwerks bis zum seriellen Port verfolgen.
- Sie können eine Mindestanzahl von IP-Adressen für PPP festlegen.
- Sie können die IP-Filterung einfacher verwalten.

Zuweisen von statischen IP-Adressen für Anrufer

Wenn an Ihrem Standort eine PPP-Authentifizierung durchgeführt wird, können Sie einzelnen Anrufern spezielle *statische* IP-Adressen zuweisen. In diesem Szenario erhält der Anrufer jedesmal dann dieselbe IP-Adresse, wenn der Einwahlserver von einem Hinauswahlrechner angewählt wird.

Sie können statische Adressen entweder in den PAP-Geheimnissen oder in der CHAP-Geheimnisdatenbank implementieren. Es folgt ein Beispiel einer `/etc/ppp/pap-secrets`-Datei, die zum Definieren von statischen IP-Adressen dient.

```
joe    myserver  joepasswd   10.10.111.240
sally  myserver  sallypasswd 10.10.111.241
sue    myserver  suepasswd   10.10.111.242
```

Anrufer `joe`, `sally` und `sue` sind die Namen der autorisierten Anrufer.

Server	`myserver` gibt den Namen des Servers an.
Passwort	`joepasswd`, `sallypasswd` und `suepasswd` geben die Passwörter für jeden Anrufer an.
IP-Adressen	`10.10.111.240`, `10.10.111.241` und `10.10.111.242` sind die IP-Adressen, die jedem Anrufer zugewiesen werden.

Es folgt ein Beispiel einer `/etc/ppp/chap-secrets`-Datei, die zum Definieren von statischen IP-Adressen dient.

```
account1 myserver secret5748  10.10.111.244
account2 myserver secret91011 10.10.111.245
```

Anrufer	`account1` und `account2` geben die Namen der Anrufer an.
Server	`myserver` gibt den Namen des Servers für jeden Anrufer an.
Passwort	`secret5748` und `secret91011` geben das CHAP-Geheimnis für jeden Anrufer an.
IP-Adressen	`10.10.111.244` und `10.10.111.245` sind die IP-Adressen für jeden Anrufer.

Zuweisen von IP-Adressen durch eine sppp-Einheitennummer

Wenn Sie die PAP- oder die CHAP-Authentifizierung verwenden, können Sie Anrufern IP-Adressen entsprechend der `sppp`-Einheitennummer zuweisen. Es folgt ein Beispiel.

```
myclient ISP-server mypassword 10.10.111.240/28+
```

Das Pluszeichen (+) zeigt an, dass die Einheitennummer der IP-Adresse hinzugefügt wird. Beachten Sie Folgendes:

- Die Adressen `10.10.111.240` bis `10.10.111.255` werden Remote-Benutzern zugewiesen.
- `sppp0` ruft die IP-Adresse `10.10.111.240` ab.
- `sppp1` ruft die IP-Adresse `10.10.111.241` ab und so weiter.

Erstellen von PPPoE-Tunneln für DSL-Unterstützung

Mithilfe von PPPoE können Sie PPP über digitale Hochgeschwindigkeitsservices für mehrere Clients bereitstellen, die ein oder mehrere DSL-Modems verwenden. PPPoE implementiert diese Services, indem ein Ethernet-Tunnel erstellt wird, der durch drei Teilnehmer führt: das Unternehmen, die Telefongesellschaft und den Serviceprovider.

- Eine Übersicht und eine Beschreibung, wie PPPoE funktioniert, finden Sie unter „PPPoE – Übersicht“ auf Seite 434.
- Aufgaben zum Einrichten von PPPoE-Tunneln finden Sie in Kapitel 20, „Einrichten eines PPPoE-Tunnels (Aufgaben)“.

Dieser Abschnitt enthält ausführliche Informationen zu PPPoE-Befehlen und -Dateien, die in der folgenden Tabelle zusammengefasst sind.

TABELLE 22–2 PPPoE-Befehle und -Konfigurationsdateien

Datei oder Befehl	Beschreibung	Siehe
`/etc/ppp/pppoe`	Eine Datei, in der Eigenschaften enthalten sind, die standardmäßig auf alle Tunnel angewendet werden, die durch PPP auf dem System eingerichtet wurden	„`/etc/ppp/pppoe`-Datei“ auf Seite 562
`/etc/ppp/pppoe.`*device*	Eine Datei, in der Eigenschaften einer bestimmten Schnittstelle enthalten sind, die von PPP für einen Tunnel verwendet wird	„`/etc/ppp/pppoe.` *device*-Datei“ auf Seite 564
`/etc/ppp/pppoe.if`	Eine Datei, in der die Ethernet-Schnittstelle aufgeführt ist, über die der Tunnel ausgeführt wird, der von PPPoE eingerichtet wurde	„`/etc/ppp/pppoe.if`-Datei“ auf Seite 559
`/usr/sbin/sppptun`	Befehl zum Konfigurieren der Ethernet-Schnittstellen, die für einen PPPoE-Tunnel benötigt werden	„`/usr/sbin/sppptun`-Befehl“ auf Seite 560
`/usr/lib/inet/pppoed`	Befehl und Optionen zur Verwendung von PPPoE, um einen Tunnel einzurichten	„`/usr/lib/inet/pppoed`-Dämon“ auf Seite 561

Dateien zum Konfigurieren von Schnittstellen für PPPoE

Damit der Tunnel die PPP-Kommunikation unterstützen kann, müssen zunächst die Schnittstellen konfiguriert werden, die sich an beiden Enden des PPPoE-Tunnels befinden. Verwenden Sie zu diesem Zweck die Dateien `/usr/sbin/sppptun` und `/etc/ppp/pppoe.if`. Sie müssen diese Tools verwenden, um die Ethernet-Schnittstellen auf allen Solaris-PPPoE-Clients und PPPoE-Zugangsservern zu konfigurieren.

`/etc/ppp/pppoe.if`-Datei

Die `/etc/ppp/pppoe.if`-Datei dient zum Auflisten der Namen aller Ethernet-Schnittstellen eines Hosts, die für die PPPoE-Tunnel verwendet werden. Diese Datei wird während des Boot-Vorgangs verarbeitet, sobald die aufgelisteten Schnittstellen für die PPPoE-Tunnel angebunden sind.

Sie müssen die Datei `/etc/ppp/pppoe.if` explizit erstellen. Geben Sie den Namen einer Schnittstelle ein, die für PPPoE je Verbindung konfiguriert werden soll.

Das folgende Beispiel zeigt eine `/etc/ppp/pppoe.if`-Datei für einen Server mit drei Schnittstellen für PPPoE-Tunnel:

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

PPPoE-Clients haben normalerweise nur eine Schnittstelle, die in `/etc/ppp/pppoe.if` angegeben ist.

`/usr/sbin/sppptun`-Befehl

Sie können den `/usr/sbin/sppptun`-Befehl verwenden, um die Ethernet-Schnittstellen, die für PPPoE-Tunnel verwendet werden sollen, manuell anzubinden oder die Anbindung manuell zu lösen. Im Gegensatz dazu wird `/etc/ppp/pppoe.if` nur dann gelesen, wenn das System gebootet wird. Diese Schnittstellen sollten den Schnittstellen entsprechen, die in `/etc/ppp/pppoe.if` aufgelistet sind.

`sppptun` dient zum Anbinden der Ethernet-Schnittstellen, die in PPPoE-Tunneln auf eine Weise verwendet werden, die der Ausführung des `ifconfig`-Befehls ähnlich ist. Anders als bei `ifconfig` müssen Sie Schnittstellen zweimal anbinden, um PPPoE zu unterstützen, weil zwei Ethernet-Protokollnummern einbezogen werden müssen.

Es folgt die grundlegende Syntax für `sppptun`:

```
# /usr/sbin/sppptun plumb pppoed device-name
      device-name:pppoed
# /usr/sbin/sppptun plumb pppoe device-name
      device-name:pppoe
```

In dieser Syntax ist *device-name* der Name des Geräts, das für PPPoE angebunden werden soll.

Wenn Sie den `sppptun`-Befehl zum ersten Mal ausführen, wird das Erkennungsprotokoll `pppoed` an die Schnittstelle angebunden. Wenn Sie den `sppptun`-Befehl zum zweiten Mal ausführen, wird das Sitzungsprotokoll `pppoe` angebunden. `sppptun` gibt den Namen der Schnittstelle aus, die gerade angebunden wurde. Diesen Namen können Sie verwenden, um die Anbindung der Schnittstelle zu lösen.

Weitere Informationen finden Sie auf der Manpage `sppptun(1M)`.

Beispiele für `sppptun`-Befehle zum Verwalten von Schnittstellen

Das folgende Beispiel zeigt, wie eine Schnittstelle für PPPoE mithilfe von `/usr/sbin/sppptun` manuell angebunden wird.

```
# /usr/sbin/sppptun plumb pppoed hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
 hme0:pppoe
```

Dieses Beispiel zeigt, wie die Schnittstellen eines Zugangsservers aufgelistet werden, der für PPPoE angebunden wurde.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

Das folgende Beispiel zeigt, wie die Anbindung einer Schnittstelle gelöst wird:

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

Befehle und Dateien für den PPPoE-Zugangsserver

Ein Serviceprovider, der seinen Kunden DSL-Services oder DSL-Unterstützung anbietet, kann einen Zugangsserver verwenden, auf dem Solaris PPPoE ausgeführt wird. Der PPPoE-Zugangsserver und der Client funktionieren nicht wie bei einer herkömmlichen Client-Server-Beziehung. Die Beziehung ähnelt der Beziehung zwischen dem Hinauswahlrechner und dem Einwahlserver bei einer Wählverbindung. Ein PPPoE-System initiiert die Kommunikation und ein anderes PPPoE-System antwortet. Im Gegensatz dazu hat das PPP-Protokoll keine Kenntnis von der Client-Server-Beziehung. PPP betrachtet beide Systeme als gleichrangige Peers.

Folgende Befehle und Dateien dienen zum Einrichten eines PPPoE-Zugangsservers:

- „`/usr/sbin/sppptun`-Befehl“ auf Seite 560
- „`/usr/lib/inet/pppoed`-Dämon“ auf Seite 561
- „`/etc/ppp/pppoe`-Datei“ auf Seite 562
- „`/etc/ppp/pppoe.` *device*-Datei“ auf Seite 564
- „Gemeinsam genutztes `pppoe.so`-Objekt“ auf Seite 567

`/usr/lib/inet/pppoed`-Dämon

Der `pppoed`-Dämon akzeptiert Broadcasts für Services von potenziellen PPPoE-Clients. Außerdem handelt `pppoed` die Serverseite des PPPoE-Tunnels aus und führt `pppd`, den PPP-Dämon, über diesen Tunnel aus.

Die `pppoed`-Services werden in den `/etc/ppp/pppoe` - und `/etc/ppp/pppoe.`*device*-Dateien konfiguriert. Wenn `/etc/ppp/pppoe` vorhanden ist, während der Boot-Vorgang ausgeführt

wird, wird pppoed automatisch ausgeführt. Sie können auch den pppoed-Dämon explizit in der Befehlszeile ausführen, indem Sie /usr/lib/inet/pppoed eingeben.

/etc/ppp/pppoe-Datei

In der /etc/ppp/pppoe-Datei werden die von einem Zugangsserver angebotenen Services beschrieben, sowie die Optionen, die definieren, wie PPP über den PPPoE-Tunnel ausgeführt wird. Sie können Services für einzelne Schnittstellen definieren, oder global, d. h. für alle Schnittstellen des Zugangsservers. Der Zugangsserver sendet die Informationen in der /etc/ppp/pppoe-Datei als Antwort auf ein Broadcast von einem potenziellen PPPoE-Client.

Es folgt die grundlegende Syntax von /etc/ppp/pppoe:

global-options
service service-name
    service-specific-options
    device interface-name

Die Parameter haben folgende Bedeutungen:

global-options — Legt die standardmäßigen Optionen für die /etc/ppp/pppoe-Datei fest. Diese Optionen können Optionen sein, die über pppoed oder pppd verfügbar sind. Eine vollständige Liste der Optionen finden Sie auf den Manpages pppoed(1M) und pppd(1M).

Beispielsweise müssen Sie die Ethernet-Schnittstellen auflisten, die für den PPPoE-Tunnel als Teil der *global options* zur Verfügung stehen. Wenn Sie keine Geräte in /etc/ppp/pppoe definieren, werden keine Services an den Schnittstellen angeboten.

Um devices als globale Option zu definieren, verwenden Sie die folgende Syntax:

device interface <,interface>

interface gibt die Schnittstelle an, die der Service auf potenzielle PPPoE-Clients hin überwacht. Wenn dem Service mehrere Schnittstellen zugewiesen sind, trennen Sie jeden Namen durch ein Komma.

service service-name — Startet die Definition des Service *service-name*. *service-name* ist eine Zeichenfolge, die ein beliebiger Ausdruck für die bereitgestellten Services sein kann.

service-specific-options — Listet die PPPoE- und PPP-Optionen auf, die für diesen Service bestimmt sind.

device *interface-name* — Gibt die Schnittstelle an, an der der zuvor angegebene Service verfügbar ist.

Weitere Optionen zu `/etc/ppp/pppoe` finden Sie auf den Manpages `pppoed(1M)` und `pppd(1M)`.

Eine typische `/etc/ppp/pppoe`-Datei kann wie folgt aussehen.

BEISPIEL 22–2 Grundlegende `/etc/ppp/pppoe`-Datei

```
device hme1,hme2,hme3
service internet
   pppd "name internet-server"
service intranet
   pppd "192.168.1.1:"
service debug
   device hme1
   pppd "debug name internet-server"
```

In dieser Datei gelten die folgenden Werte:

`hme1,hme2,hme3`	Drei Schnittstellen am Zugangsserver, die für PPPoE-Tunnel verwendet werden sollen
`service internet`	Gibt einen Service namens `internet` für potenzielle Clients bekannt. Der Provider, der den Service anbietet, bestimmt auch, wie `internet` definiert wird. Ein Provider kann beispielsweise `internet` als verschiedene IP-Services oder auch als Zugang zum Internet interpretieren.
`pppd`	Legt die Befehlszeilenoptionen fest, die verwendet werden, wenn der Anrufer `pppd` aufruft. Die Option `"name internet-server"` gibt den Namen des lokalen Rechners (Zugangsserver) als `internet-server` an.
`service intranet`	Gibt einen weiteren Service namens `intranet` für potenzielle Clients bekannt.
`pppd "192.168.1.1:"`	Legt die Befehlszeilenoptionen fest, die verwendet werden, wenn der Anrufer `pppd` aufruft. Wenn der Anrufer `pppd` aufruft, wird 192.168.1.1 als IP-Adresse für den lokalen Rechner (Zugangsserver) festgelegt.
`service debug`	Gibt einen dritten Service (Fehlersuche) für die Schnittstellen bekannt, die für PPPoE definiert sind.
`device hme1`	Beschränkt die Fehlersuche für PPPoE-Tunnel auf `hme1`.

`pppd "debug name internet-server"`	Legt die Befehlszeilenoptionen fest, die verwendet werden, wenn der Anrufer `pppd` aufruft. In diesem Fall handelt es sich um die PPP-Fehlersuche auf `internet-server` , dem lokalen Rechner.

`/etc/ppp/pppoe.` *device*-Datei

In der `/etc/ppp/pppoe.` *device*-Datei werden die Services beschrieben, die an einer Schnittstelle eines PPPoE-Zugangsservers angeboten werden. Die `/etc/ppp/pppoe.` *device*-Datei enthält zudem Optionen, die definieren, wie PPP über den PPPoE-Tunnel ausgeführt wird. Die `/etc/ppp/pppoe.` *device* ist eine optionale Datei, die genau wie `/etc/ppp/pppoe` funktioniert. Wenn die Datei `/etc/ppp/pppoe.` *device* jedoch für eine Schnittstelle definiert wird, haben die Parameter der Datei Vorrang vor den globalen Parametern, die in `/etc/ppp/pppoe` definiert sind.

Es folgt die grundlegende Syntax von `/etc/ppp/pppoe.` *device*:

```
service service-name
      service-specific-options
service another-service-name
       service-specific-options
```

Der einzige Unterschied zwischen dieser Syntax und der Syntax von `/etc/ppp/pppoe` besteht darin, dass Sie nicht die `device`-Option verwenden können, die unter „`/etc/ppp/pppoe`-Datei“ auf Seite 562 aufgeführt ist.

`pppoe.so`-Plugin

`pppoe.so` ist eine gemeinsam genutzte PPPoE-Objektdatei, die von PPPoE-Zugangsservern und -Clients aufgerufen werden muss. Diese Datei beschränkt MTU und MRU auf 1492, filtert vom Treiber kommende Pakete und handelt den PPPoE-Tunnel zusammen mit `pppoed` aus. Auf der Zugangsserverseite wird `pppoe.so` automatisch vom `pppd`-Dämon aufgerufen.

Verwenden von PPPoE- und PPP-Dateien zur Konfiguration eines Zugangsserver

Dieser Abschnitt enthält Beispiele für alle Dateien, die verwendet werden, um einen Zugangsserver zu konfigurieren. Der Zugangsserver hat mehrere Netzanbindungen. Der Server ist an drei Teilnetze angebunden: `green`, `orange` und `purple`. `pppoed` wird als `root` auf dem Server ausgeführt. Dies ist die Standardeinstellung.

PPPoE-Clients können auf die Netzwerke `orange` und `purple` über die Schnittstellen `hme0` und `hme1` zugreifen. Clients melden sich beim Server an, indem die standardmäßige UNIX-Anmeldung verwendet wird. Der Server authentifiziert die Clients mithilfe von PAP.

Das Netzwerk `green` wird gegenüber den Clients nicht bekannt gegeben. Die einzige Möglichkeit, die Clients haben, um auf `green` zuzugreifen, besteht darin, `green-net` direkt anzugeben und CHAP-Authentifizierungs-Berechtigungsnachweisen bereitzustellen. Außerdem ist nur den Clients `joe` und `mary` erlaubt, mithilfe von statischen IP-Adressen auf das Netzwerk `green` zuzugreifen.

BEISPIEL 22–3 `/etc/ppp/pppoe`-Datei für einen Zugangsserver

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
service purple-net
     device hme0,hme1
     pppd "require-pap login name purple-server purple-server:"
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

In diesem Beispiel werden die Services beschrieben, die vom Zugangsserver zur Verfügung gestellt werden. Im ersten Abschnitt werden die Services des Netzwerks `orange` beschrieben.

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
```

Die Clients können auf das Netzwerk `orange` über die Schnittstellen `hme0` und `hme1` zugreifen. Die für den `pppd`-Befehl angegebenen Optionen zwingen den Server, bei potenziellen Clients PAP-Berechtigungsnachweise anzufordern. Durch die `pppd`-Optionen wird der Name des Servers zudem auf `orange-server` festgelegt. Dadurch stimmt der Name mit dem in der `pap-secrets`-Datei verwendeten Namen überein.

Der Serviceabschnitt für das Netzwerk `purple` stimmt mit Ausnahme der Netzwerk- und Servernamen mit dem Serviceabschnitt des Netzwerks `orange` überein.

Im folgenden Abschnitt werden die Services des Netzwerks `green` beschrieben:

```
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

In diesem Abschnitt wird der Clientzugriff auf die Schnittstelle `hme1` beschränkt. Die für den `pppd`-Befehl angegebenen Optionen zwingen den Server, bei potenziellen Clients CHAP-Berechtigungsnachweise anzufordern. Durch die `pppd`-Optionen wird zudem der Name des Servers auf `green-server` festgelegt. Dieser Name wird in der `chap-secrets`-Datei verwendet. Die `nowildcard`-Option gibt an, dass das Vorhandensein des Netzwerks green den Clients nicht bekannt gegeben wird.

Für das gerade erläuterte Zugangsserverszenario können Sie die folgende `/etc/ppp/options`-Datei einrichten.

BEISPIEL 22–4 `/etc/ppp/options`-Datei für einen Zugangsserver

```
auth
proxyarp
nodefaultroute
name no-service    # don't authenticate otherwise
```

Die Option `name no-service` setzt den Servernamen außer Kraft, nach dem normalerweise während einer PAP- oder CHAP-Authentifizierung gesucht wird. Der standardmäßige Name des Servers ist der Name, der mithilfe des `/usr/bin/hostname`-Befehls gesucht wird. Die im vorangegangenen Beispiel aufgeführte `name`-Option dient zum Ändern des Servernamens in `no-service`. Es ist unwahrscheinlich, dass der Name `no-service` in einer `pap`- oder `chap-secrets`-Datei gefunden wird. Dadurch wird verhindert, dass ein Benutzer unbeabsichtigt `pppd` ausführt und die `auth`- und `name`-Optionen außer Kraft setzt, die in `/etc/ppp/options` festgelegt sind. `pppd` schlägt dann fehl, da keine Geheimnisse für den Client mit dem Servernamen `no-service` gefunden werden können.

Im Zugangsserverszenario wird die folgende `/etc/hosts`-Datei verwendet.

BEISPIEL 22–5 `/etc/hosts`-Datei für einen Zugangsserver

```
172.16.0.1    orange-server
172.17.0.1    purple-server
172.18.0.1    green-server
172.18.0.2    joes-pc
172.18.0.3    marys-pc
```

Es folgt die `/etc/ppp/pap-secrets`-Datei, die zur PAP-Authentifizierung für Clients verwendet wird, die versuchen, auf die Netzwerke `orange` und `purple` zuzugreifen.

BEISPIEL 22–6 `/etc/ppp/pap-secrets`-Datei für einen Zugangsserver

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

Es folgt die `/etc/ppp/chap-secrets`-Datei, die für die CHAP-Authentifizierung verwendet wird. Beachten Sie, dass nur die Clients `joe` und `mary` in der Datei aufgeführt sind.

BEISPIEL 22–7 `/etc/ppp/chap-secrets`-Datei für einen Zugangsserver

```
 joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

Befehle und Dateien für den PPPoE-Client

Um PPP über ein DSL-Modem auszuführen, muss ein Rechner als PPPoE-Client fungieren. Um PPPoE auszuführen, müssen Sie eine Schnittstelle anbinden und dann das `pppoec`-Dienstprogramm verwenden, um festzustellen, ob ein Zugangsserver verfügbar ist. Anschließend kann der Client den PPPoE-Tunnel über das DSL-Modem erstellen und PPP ausführen.

Der PPPoE-Client ist dem Zugangsserver zugeordnet. Dies entspricht dem herkömmlichen Client-Server-Modell. Der PPPoE-Tunnel ist keine Wählverbindung, wird aber in ähnlicher Weise konfiguriert und verwendet.

Folgende Befehle und Dateien dienen zum Einrichten eines PPPoE-Clients:

- „`/usr/sbin/sppptun`-Befehl“ auf Seite 560
- „`/usr/lib/inet/pppoec`-Dienstprogramm“ auf Seite 567
- „Gemeinsam genutztes `pppoe.so`-Objekt“ auf Seite 567
- „`/etc/ppp/peers/` *peer-name*-Datei“ auf Seite 535
- „`/etc/ppp/options`-Konfigurationsdatei“ auf Seite 530

`/usr/lib/inet/pppoec`-Dienstprogramm

Das `/usr/lib/inet/pppoec`-Dienstprogramm dient zum Aushandeln der Clientseite eines PPPoE-Tunnels. `pppoec` ist dem `chat`-Dienstprogramm ähnlich. Sie können `pppoec` nicht direkt aufrufen. Starten Sie stattdessen `/usr/lib/inet/pppoec` als Argument für die `connect`-Option von `pppd`.

Gemeinsam genutztes `pppoe.so`-Objekt

`pppoe.so` ist das gemeinsam genutzte PPPoE-Objekt, das von PPPoE geladen werden muss, um die PPPoE-Funktionen für Zugangsserver und Clients bereitzustellen. Das gemeinsam genutzte `pppoe.so`-Objekt beschränkt MTU und MRU auf 1492, filtert vom Treiber kommende Pakete und bearbeitet laufzeitbezogene PPPoE-Meldungen.

Auf der Clientseite lädt `pppd` das gemeinsam genutzte Objekt `pppoe.so`, wenn der Benutzer die `plugin pppoe.so`-Option angibt.

`/etc/ppp/peers/` *peer-name*-Datei zum Definieren eines Zugangsserver-Peers

Wenn Sie einen Zugangsserver definieren, der von `pppoec` erkannt werden soll, verwenden Sie die Optionen, die für `pppoec` und den `pppd` -Dämon gleichermaßen gelten. Eine `/etc/ppp/peers/`*peer-name*-Datei für einen Zugangsserver erfordert die folgenden Parameter:

- `sppptun` – Name für das serielle Gerät, das vom PPPoE-Tunnel verwendet wird
- `plugin pppoe.so` – weist `pppd` an, das gemeinsam genutzte `pppoe.so`-Objekt zu laden.
- `connect "/usr/lib/inet/pppoec` *device* `"` – initiiert eine Verbindung. `connect` ruft dann das `pppoec`-Dienstprogramm über die für PPPoE angebundene Schnittstelle (*device*) auf.

Die übrigen Parameter in der `/etc/ppp/peers/` *peer-name*-Datei gelten für die PPP-Verbindung des Servers. Verwenden Sie dieselben Optionen wie für `/etc/ppp/peers/` *peer-name* auf dem Hinauswahlrechner. Versuchen Sie, die Anzahl der Optionen auf ein Minimum zu beschränken, das für die PPP-Verbindung ausreicht.

Das folgende Beispiel wird unter „So definieren Sie einen PPPoE-Zugangsserver-Peer“ auf Seite 498 vorgestellt.

BEISPIEL 22–8 `/etc/ppp/peers/` *peer-name* zum Definieren eines Remote-Zugangsservers

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

Mithilfe dieser Datei werden die Parameter definiert, die verwendet werden, wenn ein PPPoE-Tunnel und eine PPP-Verbindung eingerichtet werden, um den Zugriff auf den Server `dslserve` zu ermöglichen. Dabei werden die nachstehenden Optionen verwendet.

Option	Beschreibung
`sppptun`	Definiert `sppptun` als Name für das serielle Gerät.
`plugin pppoe.so`	Weist `pppd` an, das gemeinsam genutzte `pppoe.so`-Objekt zu laden.
`connect "/usr/lib/inet/pppoec hme0"`	Führt `pppoec` aus und legt `hme0` als Schnittstelle für den PPPoE-Tunnel und die PPP-Verbindung fest.

Option	Beschreibung
`noccp`	Deaktiviert die CCP-Komprimierung der Verbindung. **Hinweis –** Viele ISPs verwenden nur spezifische Komprimierungsalgorithmen. Durch die Deaktivierung der öffentlich verfügbaren CCP-Algorithmen wird weniger Zeit für die Aushandlung benötigt, und es werden gelegentliche Interoperabilitätsprobleme vermieden.
`noauth`	Bewirkt, dass `pppd` keine Authentifizierungs-Berechtigungsnachweise mehr beim Zugangsserver anfordert werden. Die meisten ISPs stellen keine Authentifizierungs-Berechtigungsnachweise für Kunden bereit.
`user Red`	Legt den Namen `Red` als Benutzernamen für den Client fest. Dieser Name wird vom Zugangsserver für die PAP-Authentifizierung benötigt.
`password redsecret`	Legt `redsecret` als Passwort fest, das an den Zugangsserver für die PAP-Authentifizierung weitergegeben wird.
`noipdefault`	Weist 0.0.0.0 als anfängliche IP-Adresse zu.
`defaultroute`	Teilt `pppd` mit, nach der IPCP-Aushandlung eine standardmäßige IPv4-Route zu installieren. Sie sollten `defaultroute` in `/etc/ppp/peers/`*peer-name* einbeziehen, wenn es sich bei der Verbindung um die Verbindung des Systems mit dem Internet handelt, die für einen PPPoE-Client gültig ist.

◆ ◆ ◆ KAPITEL 23

Migrieren von Asynchronous Solaris PPP zu Solaris PPP 4.0 (Aufgaben)

Frühere Versionen des Betriebssystems Solaris enthielten eine andere PPP-Implementierung – Asynchronous Solaris PPP (`asppp`). Wenn Sie Peers, die `asppp` ausführen, auf das neuere PPP 4.0 umstellen möchten, müssen Sie ein Konvertierungsskript ausführen. Dieses Kapitel enthält folgende Themen zur PPP-Konvertierung:

- „Vor dem Konvertieren von `asppp`-Dateien“ auf Seite 571
- „Ausführen des `asppp2pppd`-Konvertierungsskripts (Aufgaben)“ auf Seite 574

Anhand einer `asppp`-Beispielkonfiguration wird erläutert, wie die PPP-Konvertierung durchgeführt wird. Eine Beschreibung der Unterschiede zwischen Solaris PPP 4.0 und `asppp` finden Sie unter „Zu verwendende Version von Solaris PPP“ auf Seite 422.

Vor dem Konvertieren von `asppp`-Dateien

Mithilfe des Konvertierungsskripts `/usr/sbin/asppp2pppd` können Sie die Dateien konvertieren, aus denen eine standardmäßige `asppp`-Konfiguration besteht:

- `/etc/asppp.cf` – Konfigurationsdatei für Asynchronous PPP
- `/etc/uucp/Systems` – UUCP-Datei, in der die Merkmale des Remote-Peers beschrieben sind
- `/etc/uucp/Devices` – UUCP-Datei, in der das Modem des lokalen Rechners beschrieben ist
- `/etc/uucp/Dialers` – UUCP-Datei, in der die Anmeldesequenz enthalten ist, die von dem Modem verwendet wird, das in der `/etc/uucp/Devices`-Datei beschrieben ist

Weitere Informationen zu `asppp` finden Sie in *Solaris 8 System Administration Collection, Volume 3* unter `http://docs.sun.com`.

Beispiel für eine /etc/asppp.cf -Konfigurationsdatei

Im unter „So konvertieren Sie von asppp in Solaris PPP 4.0“ auf Seite 575 beschriebenen Verfahren wird die folgende /etc/asppp.cf-Datei verwendet:

```
#
ifconfig ipdptp0 plumb mojave gobi up

path
 inactivity_timeout 120     # Approx. 2 minutes
    interface ipdptp0
    peer_system_name Pgobi    # The name we log in with (also in
                                    # /etc/uucp/Systems
```

Die Datei enthält folgende Parameter:

`ifconfig ipdptp0 plumb mojave gobi up`	Führt den Befehl `ifconfig` aus, um eine Verbindung von der PPP-Schnittstelle `ipdptp0` auf dem lokalen Rechner `mojave` zum Remote-Peer `gobi` zu konfigurieren.
`inactivity_timeout 120`	Unterbricht die Leitung nach zwei Minuten Inaktivität.
`interface ipdptp0`	Konfiguriert die Schnittstelle `ipdptp0` auf dem Hinauswahlrechner für asynchrones PPP.
`peer_system_name Pgobi`	Gibt den Namen des Remote-Peers, `Pgobi`, an.

Beispiel für die /etc/uucp/Systems -Datei

In dem unter „So konvertieren Sie von asppp in Solaris PPP 4.0“ auf Seite 575 beschriebenen Verfahren wird die folgende /etc/uucp/Systems-Datei verwendet:

```
#ident  "@(#)Systems    1.5  92/07/14 SMI"  /* from SVR4 bnu:Systems 2.4 */
#

# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojave word: sand
```

Die Datei enthält folgende Parameter:

`Pgobi`	Verwendet `Pgobi` als Hostname des Remote-Peers.
`Any ACU`	Teilt dem Modem des Hinauswahlrechners `mojave` mit, zu einer beliebigen Tageszeit eine Verbindung mit einem Modem auf `Pgobi` herzustellen. "Any ACU" bedeutet "nach ACU in der /etc/uucp/Devices-Datei suchen".

`38400`	Legt 38400 als Höchstgeschwindigkeit der Verbindung fest.
`15551212`	Gibt die Telefonnummer von `Pgobi` an.
`in:–in: mojave word: sand`	Definiert das Anmeldeskript, das von `Pgobi` benötigt wird, um den Hinauswahlrechner `mojave` zu authentifizieren.

Beispiel für die `/etc/uucp/Devices` -Datei

Im unter „So konvertieren Sie von asppp in Solaris PPP 4.0“ auf Seite 575 beschriebenen Verfahren wird die folgende `/etc/uucp/Devices`-Datei verwendet:

```
#ident  "@(#)Devices  1.6  92/07/14 SMI"  /* from SVR4 bnu:Devices 2.7 */

.
.
#

TCP,et - - Any TCP -
.
.
#
ACU cua/b - Any hayes
# 0-7 are on a Magma 8 port card
Direct cua/0 - Any direct
Direct cua/1 - Any direct
Direct cua/2 - Any direct
Direct cua/3 - Any direct
Direct cua/4 - Any direct
Direct cua/5 - Any direct
Direct cua/6 - Any direct
Direct cua/7 - Any direct
# a is the console port (aka "tip" line)
Direct cua/a - Any direct
# b is the aux port on the motherboard
Direct cua/b - Any direct
# c and d are high speed sync/async ports
Direct cua/c - Any direct
Direct cua/d - Any direct
```

Die Datei dient zur Unterstützung von Hayes-Modems, die mit dem seriellen Port `cua/b` verbunden sind.

Beispiel für die `/etc/uucp/Dialers` -Datei

Im unter „So konvertieren Sie von asppp in Solaris PPP 4.0“ auf Seite 575 beschriebenen Verfahren wird die folgende `/etc/uucp/Dialers`-Datei verwendet:

```
#
#       <Much information about modems supported by Oracle Solaris UUCP>
```

```
penril    =W-P    "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
ventel    =&-%    "" \r\p\r\c $ k\c ONLINE!
vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE
develcon ""    "" \pr\ps\c est:\007 \E\D\e \n\007
micom    ""    "" \s\c NAME? \D\r\c GO
direct
#
#
#
#   Hayes Smartmodem -- modem should be set with the configuration
#   switches as follows:
#
#       S1 - UP        S2 - UP        S3 - DOWN    S4 - UP
#       S5 - UP        S6 - DOWN    S7 - ?        S8 - DOWN
#
hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT
```

<much more information about modems supported by Oraccle Solaris UUCP>

Diese Datei enthält die Chat-Skripten für alle Modemtypen, einschließlich Hayes-Modems, die in der `/etc/uucp/Dialers`-Datei unterstützt werden.

Ausführen des `asppp2pppd`-Konvertierungsskripts (Aufgaben)

Das `/usr/sbin/asppp2pppd`-Skript kopiert die PPP-Informationen in `/etc/asppp.cf` - und PPP-bezogenen UUCP-Dateien an die entsprechenden Stellen in den Solaris PPP 4.0-Dateien.

Voraussetzungen

Bevor Sie zur nächsten Aufgabe übergehen, führen Sie Folgendes aus:

- Installieren Sie Solaris auf dem Rechner, auf dem sich die `asppp`- und UUCP-Konfigurationsdateien befinden.
- Melden Sie sich als Superuser beim Rechner mit den PPP-Dateien an, beispielsweise beim Rechner `mojave`.

▼ So konvertieren Sie von asppp in Solaris PPP 4.0

1 Starten Sie das Konvertierungsskript.

```
# /usr/sbin/asppp2pppd
```

Die Konvertierung wird gestartet, und folgende Bildschirmausgabe wird angezeigt:

```
This script provides only a suggested translation for your existing aspppd
configuration.  You will need to evaluate for yourself whether the translation
is appropriate for your operating environment.
Continue [Yn]?
```

2 Geben Sie "Y" ein, um fortzufahren.

Folgende Bildschirmausgabe wird angezeigt:

```
Chat cannot do echo checking; requests for this removed.
Adding 'noauth' to /etc/ppp/options

Preparing to write out translated configuration:
    1 chat file:
        1.  /etc/ppp/chat.Pgobi.hayes
    2 option files:
        2.  /etc/ppp/peers/Pgobi
        3.  /etc/ppp/options
    1 script file:
        4.  /etc/ppp/demand
```

Die neuen Solaris PPP 4.0-Dateien wurden erstellt.

▼ So zeigen Sie die Ergebnisse der Konvertierung an

Sie können die Solaris PPP 4.0-Dateien anzeigen, die mithilfe des `/usr/sbin/asppp2pppd`-Konvertierungsskripts am Ende des Konvertierungsvorgangs erstellt wurden. Das Skript zeigt die folgende Liste von Optionen an.

```
Enter option number:
        1 - view contents of file on standard output
        2 - view contents of file using /usr/bin/less
        3 - edit contents of file using /usr/bin/vi
        4 - delete/undelete file from list
        5 - rename file in list
        6 - show file list again
        7 - escape to shell (or "!")
        8 - abort without saving anything
        9 - save all files and exit (default)
Option:
```

1 Geben Sie 1 ein, um die Inhalte der Dateien auf dem Bildschirm anzuzeigen.

Das Skript fordert die Nummer der Datei an, die Sie anzeigen möchten.

```
File number (1 .. 4):
```

Die Nummern beziehen sich auf die umgesetzten Dateien, die während der Konvertierung aufgelistet werden (siehe Schritt 2 oben).

2 Geben Sie 1 ein, um die Chat-Datei `/etc/ppp/chat.Pgobi.hayes` anzuzeigen.

```
File number (1 .. 4):  1
"" \d\dA\p\pTE1V1X1Q0S2=255S12=255\r\c
OK\r ATDT\T\r\c
CONNECT \c
in:--in: mojave
word: sand
```

Das Chat-Skript enthält die Chat-Modeminformationen, die in der hayes-Zeile in der Beispieldatei `/etc/uucp/Dialers` angezeigt werden. `/etc/ppp/chat.Pgobi.hayes` enthält zudem die Anmeldesequenz für `Pgobi`, die in der Beispieldatei `/etc/uucp/Systems` zu finden ist. Das Chat-Skript befindet sich nun in der Datei `/etc/ppp/chat.Pgobi.hayes` .

3 Geben Sie 2 ein, um die Peers-Datei `/etc/ppp/peers/Pgobi` anzuzeigen.

```
File number (1 .. 4):  2
/dev/cua/b
38400
demand
idle 120
connect "/usr/bin/chat -f /etc/ppp/chat.Pgobi.hayes -T '15551212'"
user NeverAuthenticate
mojave:gobi
```

Die Informationen zum seriellen Port (`/dev/cua/b`) stammen aus der Datei `/etc/uucp/Devices`. Die Verbindungsgeschwindigkeit, die Leerlaufzeit, die Authentifizierungsinformationen und die Peer-Namen stammen aus der Datei `/etc/asppp.cf`. "demand" bezieht sich auf das "demand"-Skript, das aufgerufen werden muss, wenn der Hinauswahlrechner versucht, eine Verbindung mit dem Peer `Pgobi` herzustellen.

4 Geben Sie 3 ein, um die `/etc/ppp/options`-Datei anzuzeigen, die für den Hinauswahlrechner `mojave` erstellt wird.

```
File number (1 .. 4):  3
#lock
noauth
```

Die Informationen in `/etc/ppp/options` stammen aus der Datei `/etc/asppp.cf` .

5 Geben Sie 4 ein, um den Inhalt des `demand` -Skripts anzuzeigen.

```
File number (1 .. 4):  4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

Wenn dieses Skript aufgerufen wird, führt es den Befehl pppd aus. Dadurch wird /etc/ppp/peers/Pgobi gelesen und die Verbindung zwischen mojave und Pgobi initiiert.

6 Geben Sie 9 ein, um die erstellten Dateien zu speichern. Beenden Sie dann das Konvertierungsskript.

◆ ◆ ◆ KAPITEL 24

UUCP (Übersicht)

In diesem Kapitel werden das UUCP (UNIX-to-UNIX Copy Program) und die zugehörigen Dämonen vorgestellt. Folgende Themen werden behandelt:

- „UUCP-Hardwarekonfigurationen“ auf Seite 579
- „UUCP-Software“ auf Seite 580
- „UUCP-Datenbankdateien“ auf Seite 583

Mit UUCP können Computer Dateien übertragen und untereinander Mails austauschen. Computer können mit diesem Programm auch auf große Netzwerke wie beispielsweise Usenet zugreifen.

Im Betriebssystem Solaris ist die BNU-Version (Basic Network Utilities) von UUCP integriert, die auch als HoneyDanBer-UUCP bekannt ist. Der Begriff *UUCP* umfasst sämtliche Dateien und Dienstprogramme, aus denen das System besteht, von dem das Programm `uucp` nur einen Teil darstellt. Zu den UUCP-Dienstprogrammen zählen Dienstprogramme, die zum Kopieren von Dateien zwischen Computern verwendet werden (`uucp` und `uuto`) sowie Dienstprogramme, die für die Remote-Anmeldung und zur Befehlsausführung verwendet werden (`cu` und `uux`).

UUCP-Hardwarekonfigurationen

UUCP unterstützt folgende Hardwarekonfigurationen:

Direkte Verbindungen — Sie können eine direkte Verbindung mit einem anderen Computer herstellen, indem Sie die seriellen Ports der beiden Rechner mit einem RS-232-Kabel verbinden. Direkte Verbindungen sind zweckmäßig, wenn zwei Computer regelmäßig und in kurzer Entfernung (beispielsweise 15 m) miteinander kommunizieren. Sie können ein Modem für kurze Entfernungen verwenden, um diese Entfernung etwas zu vergrößern.

Telefonleitungen	Mithilfe einer automatischen Wähleinrichtung (Automatic Call Unit, ACU), beispielsweise einem Hochgeschwindigkeitsmodem, kann Ihr Rechner über eine normale Telefonleitung mit anderen Computern kommunizieren. Das Modem wählt die Telefonnummer, die durch UUCP angefordert wird. Der empfangende Rechner muss ein Modem haben, das eingehende Aufrufe beantworten kann.
Netzwerk	UUCP kann auch über ein Netzwerk kommunizieren, in dem TCP/IP oder andere Protokolle verwendet werden. Sobald Ihr Computer als Host in einem Netzwerk eingerichtet ist, kann sich Ihr Computer mit jedem anderen Host im Netzwerk verbinden.

In diesem Kapitel wird vorausgesetzt, dass Ihre UUCP-Hardware bereits installiert und konfiguriert ist. Wenn Sie ein Modem einrichten müssen, informieren Sie sich unter *System Administration Guide: Basic Administration* und in den Modemhandbüchern.

UUCP-Software

Die UUCP-Software wird automatisch installiert, wenn Sie beim Ausführen des Solaris-Installationsprogramms die gesamte Distribution auswählen. Außerdem können Sie die UUCP-Software mithilfe von `pkgadd` hinzufügen. Bei UUCP-Programmen unterscheidet man zwischen drei Kategorien: Dämonen, Verwaltungsprogramme und Benutzerprogramme.

UUCP-Dämonen

Das UUCP-System hat vier Dämonen: `uucico`, `uuxqt`, `uusched` und `in.uucpd`. Diese Dämonen führen UUCP-Dateiübertragungen und Befehle aus. Sie können diese Dämonen auch manuell über eine Shell ausführen.

`uucico` Wählt das Gerät aus, das für die Verbindung verwendet wird, richtet die Verbindung für den Remote-Computer ein und führt die erforderliche Anmeldesequenz und Berechtigungsprüfungen durch. Außerdem überträgt `uucico` Datendateien, Ausführungsdateien und Ergebnisse aus Protokollen und benachrichtigt Benutzer per Mail über den Abschluss von Übertragungen. `uucico` fungiert als Anmelde-Shell für UUCP-Anmeldungskonten. Wenn der lokale `uucico`-Dämon einen Remote-Rechner aufruft, kommuniziert er während der Sitzung direkt mit dem `uucico`-Remote-Dämon.

Nachdem alle erforderlichen Dateien erstellt wurden, führen die `uucp`-, `uuto`- und `uux`-Programme den `uucico`-Dämon aus, um den Remote-Computer zu kontaktieren. `uusched` und `Uutry` führen `uucico` aus. Weitere Informationen finden Sie auf der Manpage `uucico(1M)`.

`uuxqt` Führt Remote-Ausführungsanforderungen aus. Dieser Dämon sucht im Spool-Verzeichnis nach Ausführungsdateien (mit der Benennung X.*file*), die von einem Remote-Computer gesendet wurden. Wenn eine X.*file*-Datei gefunden wird, wird sie von `uuxqt` geöffnet, um die Liste der Datendateien zu erhalten, die für die Ausführung erforderlich sind. `uuxqt` prüft dann, ob die erforderlichen Datendateien verfügbar und zugänglich sind. Wenn die Dateien verfügbar sind, prüft `uuxqt` die Datei `Permissions` , um sicherzustellen, dass die Berechtigungen zur Ausführung des angeforderten Befehls vorhanden sind. Der `uuxqt`-Dämon wird vom `uudemon.hour` -Shell-Skript ausgeführt, das durch `cron` gestartet wird. Weitere Informationen finden Sie auf der Manpage `uuxqt`(1M).

`uusched` Plant die Ausführung der Vorgänge, die sich in der Warteschlange im Spool-Verzeichnis befinden. `uusched` wird anfangs während des Boot-Vorgangs durch das `uudemon.hour`-Shell-Skript ausgeführt, das durch `cron` gestartet wird. Weitere Informationen finden Sie auf der Manpage `uusched`(1M). Bevor der `uucico`-Dämon gestartet wird, generiert `uusched` Zufallszahlen für die Reihenfolge, in der Remote-Computer aufgerufen werden.

`in.uucpd` Unterstützt UUCP-Verbindungen über Netzwerke. Der Dämon `inetd` auf dem Remote-Host ruft `in.uucpd` immer dann auf, wenn eine UUCP-Verbindung hergestellt wird. Von `uucpd` wird dann aufgefordert, einen Anmeldename anzugeben. `uucico` auf dem aufrufenden Host muss mit einem Anmeldenamen antworten. `in.uucpd` fordert dann zur Angabe eines Passworts auf, es sei denn, ein Passwort ist nicht erforderlich. Weitere Informationen finden Sie auf der Manpage `in.uucpd`(1M).

UUCP-Verwaltungsprogramme

Die meisten UUCP-Verwaltungsprogramme befinden sich in `/usr/lib/uucp`. Die meisten grundlegenden Datenbankdateien befinden sich in `/etc/uucp`. Die einzige Ausnahme stellt die Datei `uulog` dar, die sich in `/usr/bin` befindet. Das Home-Verzeichnis der `uucp`-Anmelde-ID ist `/usr/lib/uucp`. Verwenden Sie zum Ausführen der Verwaltungsprogramme mit `su` oder `login` die `uucp`-Benutzer-ID. Mit der Benutzer-ID kann über die Programme und gespoolten Datendateien verfügt werden.

`uulog` Zeigt den Inhalt der Protokolldateien eines bestimmten Computers an. Protokolldateien werden für jeden Remote-Computer erstellt, mit dem Ihr Rechner kommuniziert. In den Protokolldateien wird jede Verwendung von `uucp`, `uuto` und `uux` aufgezeichnet. Weitere Informationen finden Sie auf der Manpage `uucp`(1C).

`uucleanup` Bereinigt das Spool-Verzeichnis. `uucleanup` wird normalerweise vom `uudemon.cleanup`-Shell-Skript ausgeführt, das durch `cron` gestartet wird. Weitere Informationen finden Sie auf der Manpage `uucleanup`(1M).

`Uutry` Prüft Aufrufverarbeitungsfunktionen und führt eine mittlere Fehlersuche aus. `Uutry` ruft den `uucico` -Dämon auf, um eine Kommunikationsverbindung zwischen Ihrem Rechner und dem von Ihnen angegebenen Remote-Computer herzustellen. Weitere Informationen finden Sie auf der Manpage `Uutry`(1M).

`uucheck` Überprüft das Vorhandensein von UUCP-Verzeichnissen, Programmen und Unterstützungsdateien. `uucheck` kann zudem bestimmte Teile der `/etc/uucp/Permissions`-Datei auf offensichtliche Syntaxfehler prüfen. Weitere Informationen finden Sie auf der Manpage `uucheck`(1M).

UUCP-Benutzerprogramme

Die UUCP-Benutzerprogramme befinden sich in `/usr/bin`. Sie brauchen keine speziellen Berechtigungen, um diese Programme verwenden zu können.

`cu` Verbindet Ihren Rechner mit einem Remote-Computer, wodurch Sie sich gleichzeitig bei beiden Rechnern anmelden können. Mit `cu` können Sie Dateien übertragen oder auf jedem Rechner Befehle ausführen, ohne die anfängliche Verbindung zu unterbrechen. Weitere Informationen finden Sie auf der Manpage `cu`(1C).

`uucp` Ermöglicht Ihnen, eine Datei von einem Rechner auf einen anderen zu kopieren. `uucp` erstellt Arbeits- und Datendateien, stellt Jobs zur Übertragung in die Warteschlange und ruft den `uucico`-Dämon auf, der dann versucht, den Remote-Computer zu kontaktieren. Weitere Informationen finden Sie auf der Manpage `uucp`(1C).

`uuto` Kopiert Dateien vom lokalen Rechner in das öffentliche Spool-Verzeichnis `/var/spool/uucppublic/receive` auf dem Remote-Rechner. Anders als beim Befehl `uucp`, mit dem Sie eine Datei in ein zugängliches Verzeichnis auf dem Remote-Rechner kopieren können, wird mit dem Befehl `uuto` eine Datei in ein Spool-Verzeichnis kopiert und dem Remote-Benutzer mitgeteilt, die Datei mit `uupick` abzurufen. Weitere Informationen finden Sie auf der Manpage `uuto`(1C).

`uupick` Ruft Dateien aus `/var/spool/uucppublic/receive` ab, wenn Dateien mithilfe von `uuto` auf einen Computer übertragen werden. Weitere Informationen finden Sie auf der Manpage `uuto`(1C).

`uux` Erstellt die Arbeits-, Daten- und Ausführungsdateien, die benötigt werden, um Befehle auf einem Remote-Rechner auszuführen. Weitere Informationen finden Sie auf der Manpage `uux`(1C).

`uustat` Zeigt den Status von angeforderten Übertragungen an (`uucp`, `uuto` oder `uux`). `uustat` dient auch zur Steuerung von Übertragungen, die sich in der Warteschlange befinden. Weitere Informationen finden Sie auf der Manpage `uustat`(1C).

UUCP-Datenbankdateien

Ein wichtiger Teil der UUCP-Einrichtung ist die Konfiguration der Dateien, aus denen die UUCP-Datenbank besteht. Diese Dateien befinden sich im `/etc/uucp`-Verzeichnis. Sie müssen diese Dateien bearbeiten, um UUCP oder `asppp` auf Ihrem Rechner einzurichten. Es handelt es sich um folgende Dateien:

`Config` Enthält eine Liste von Variablenparametern. Sie können diese Parameter manuell definieren, um das Netzwerk zu konfigurieren.

`Devconfig` Wird zum Konfigurieren der Netzwerkkommunikation verwendet.

`Devices` Wird zum Konfigurieren der Netzwerkkommunikation verwendet.

`Dialcodes` Enthält Wählcodekürzel, die im Telefonnummernfeld der Einträge in der `Systems`-Datei verwendet werden können. Obwohl nicht erforderlich, kann `Dialcodes` auch von `asppp` und UUCP verwendet werden.

`Dialers` Enthält Zeichenfolgen, die erforderlich sind, um mit Modems zu verhandeln, um Verbindungen mit Remote-Computern herstellen zu können. `Dialers` wird von `asppp` sowie UUCP verwendet.

`Grades` Definiert Jobklassen sowie die mit jeder Jobklasse verbundenen Berechtigungen, die Benutzer angeben können, um Jobs, die für einen Remote-Computer bestimmt sind, in eine Warteschlange zu stellen.

`Limits` Definiert die maximale Anzahl der gleichzeitigen Ausführungen von `uucico`s, `uuxqt`s und `uusched`s, die auf Ihrem Rechner zugelassen sind.

`Permissions` Definiert die Ebene des Zugriffs, der Remote-Hosts gewährt wird, die versuchen, Dateien zu übertragen oder auf Ihrem Rechner Befehle auszuführen.

`Poll` Definiert Rechner, die von Ihrem System aufgerufen werden sollen, und den Zeitpunkt, wann diese Rechner aufgerufen werden sollen.

`Sysfiles` Weist verschiedene oder mehrere Dateien zu, die von `uucico` und `cu` als `Systems`-, `Devices`- und `Dialers` -Dateien verwendet werden.

`Sysname` Ermöglicht Ihnen, einen eindeutigen UUCP-Namen für einen Rechner zu definieren, der zusätzlich zu seinem TCP/IP-Hostnamen angegeben wird.

`Systems` Enthält Informationen, die vom `uucico`-Dämon sowie von `cu` und `asppp` benötigt werden, um eine Verbindung mit einem Remote-Computer herzustellen. In diesen Informationen ist Folgendes enthalten:

- Name des Remote-Hosts
- Name des verbindenden Geräts, das dem Remote-Host zugeordnet ist
- Zeit, wann der Host erreicht werden kann
- Telefonnummer

- Anmelde-ID
- Password (Passwort)

Obwohl viele andere Dateien als Teil der unterstützenden Datenbank betrachtet werden können, sind sie nicht direkt an der Herstellung einer Verbindung und der Übertragung von Dateien beteiligt.

Konfigurieren von UUCP-Datenbankdateien

Die UUCP-Datenbank besteht aus den Dateien, die unter „UUCP-Datenbankdateien“ auf Seite 583 aufgeführt sind. Jedoch werden für die grundlegende UUCP-Konfiguration nur die folgenden wichtigen Dateien benötigt:

- `/etc/uucp/Systems`
- `/etc/uucp/Devices`
- `/etc/uucp/Dialers`

Da `asppp` einige der UUCP-Datenbanken verwendet, sollten Sie sich zumindest mit diesen wichtigen Datenbankdateien vertraut machen, wenn Sie vorhaben, `asppp` zu konfigurieren. Nachdem diese Datenbanken konfiguriert wurden, gestaltet sich die UUCP-Verwaltung relativ einfach. Sie können zunächst die `Systems`-Datei und anschließend die `Devices`-Datei bearbeiten. Sie können die standardmäßige `/etc/uucp/Dialers`-Dateien verwenden, es sei denn, Sie haben vor, Dialer hinzuzufügen, die nicht in der Standarddatei enthalten sind. Außerdem können Sie die folgenden Dateien für die grundlegende Konfiguration von UUCP und `asppp` verwenden:

- `/etc/uucp/Sysfiles`
- `/etc/uucp/Dialcodes`
- `/etc/uucp/Sysname`

Da diese Dateien in enger Beziehung zueinander stehen, sollten Sie sich mit dem Inhalt dieser Dateien vertraut machen, bevor Sie Änderungen vornehmen. Eine Änderung eines Dateieintrags kann eine Änderung eines in Relation stehenden anderen Dateieintrags erfordern. Die übrigen in „UUCP-Datenbankdateien“ auf Seite 583 aufgelisteten Dateien sind hiervon weniger betroffen.

Hinweis – `asppp` verwendet nur die in diesem Abschnitt beschriebenen Dateien. `asppp` verwendet nicht die anderen UUCP-Datenbankdateien.

◆ ◆ ◆ KAPITEL 25

Verwalten von UUCP (Aufgaben)

In diesem Kapitel wird erklärt, wie UUCP-Vorgänge gestartet werden, nachdem Sie die Datenbankdatei modifiziert haben, die für Ihre Rechner relevant ist. Das Kapitel enthält Verfahren und Fehlerbehebungsinformationen zum Einrichten und Verwalten von UUCP auf Rechnern, auf denen das Betriebssystem Solaris ausgeführt wird, darunter folgende:

- „UUCP-Verwaltung (Übersicht der Schritte)“ auf Seite 585
- „Hinzufügen von UUCP-Anmeldungen“ auf Seite 586
- „Starten von UUCP“ auf Seite 587
- „Ausführen von UUCP über TCP/IP“ auf Seite 589
- „UUCP-Sicherheit und Verwaltung“ auf Seite 590
- „UUCP-Fehlerbehebung“ auf Seite 592

UUCP-Verwaltung (Übersicht der Schritte)

Die folgende Tabelle enthält Verweise auf die Verfahren, die in diesem Kapitel behandelt werden, sowie kurze Beschreibungen der Verfahren.

TABELLE 25–1 Übersicht der Schritte für die UUCP-Verwaltung

Aufgabe	Beschreibung	Siehe
Zulassen des Zugriffs auf Ihr System durch Remote-Rechner	Bearbeiten Sie die `/etc/passwd`-Datei, um Einträge einzufügen, die zum Ermitteln der Rechner dienen, die berechtigt sind, auf Ihr System zuzugreifen.	„So fügen Sie UUCP-Anmeldungen hinzu“ auf Seite 586
Starten von UUCP	Verwenden Sie die bereitgestellten Shell-Skripten, um UUCP zu starten.	„So starten Sie UUCP“ auf Seite 588
Aktivieren von UUCP für TCP/IP	Bearbeiten Sie die `/etc/inetd.conf`- und `/etc/uucp/Systems`-Dateien, um UUCP für TCP/IP zu aktivieren.	„So aktivieren Sie UUCP für TCP/IP“ auf Seite 589

TABELLE 25–1 Übersicht der Schritte für die UUCP-Verwaltung *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Beheben einiger allgemeiner UUCP-Probleme	Prüfen Sie anhand eines Diagnoseverfahrens, ob fehlerhafte Modems oder ACUs vorhanden sind.	„So stellen Sie fest, ob fehlerhafte Modems oder ACUs vorhanden sind“ auf Seite 592
	Prüfen Sie Übertragungen auf Fehler, indem Sie ein Diagnoseverfahren verwenden.	„So suchen Sie Übertragungsfehler“ auf Seite 592

Hinzufügen von UUCP-Anmeldungen

Damit von Remote-Rechnern eingehende UUCP (`uucico`)-Anforderungen ordnungsgemäß verarbeitet werden, muss jeder Rechner über eine Anmeldung für Ihr System verfügen.

▼ So fügen Sie UUCP-Anmeldungen hinzu

Damit ein Remote-Rechner auf Ihr System zugreifen kann, müssen Sie einen Eintrag in die `/etc/passwd`-Datei einfügen. Zu diesem Zweck gehen Sie wie folgt vor:

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Bearbeiten Sie die `/etc/passwd`-Datei, und fügen Sie den Eintrag ein, der zum Ermitteln des Rechners dient, der berechtigt ist, auf Ihr System zuzugreifen.**

   Ein typischer Eintrag, den Sie in die `/etc/passwd`-Dateien für einen Remote-Rechner einfügen können, dem der Zugriff auf Ihr System mithilfe einer UUCP-Verbindung erlaubt ist, hat folgendes Aussehen:

   ```
   Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
   ```

   Normalerweise ist der Anmeldename eines Remote-Rechners der Rechnername, dem der Großbuchstabe `U` vorangestellt ist. Beachten Sie, dass der Name nur aus maximal acht Zeichen bestehen darf. Anderenfalls müssen Sie den Namen kürzen oder abkürzen.

   Der vorangegangene Eintrag zeigt, dass eine Anmeldeanforderung von `Ugobi` von `/usr/lib/uucp/uucico` beantwortet wird. Das Home-Verzeichnis ist `/var/spool/uucppublic`. Das Passwort wird aus der `/etc/shadow` -abgerufen. Sie müssen das Passwort und den Anmeldenamen mit dem UUCP-Administrator des Remote-Rechners koordinieren. Der Remote-Administrator muss dann einen entsprechenden Eintrag mit einem Anmeldenamen und einem unverschlüsselten Passwort in die `Systems`-Datei des Remote-Rechners einfügen.

3 **Koordinieren Sie Ihren Rechnernamen mit den UUCP-Administratoren von anderen Systemen.**

Sie müssen auch den Namen und das Passwort Ihres Rechners mit den UUCP-Administratoren aller Rechner koordinieren, die über UUCP erreicht werden sollen.

Starten von UUCP

UUCP enthält vier Shell-Skripten, die dazu dienen, Remote-Rechner abzufragen, Übertragungen neu zu planen und alte Dateien und nicht fehlgeschlagene Übertragungen zu löschen. Folgende Skripten stehen zur Verfügung:

- `uudemon.poll`
- `uudemon.hour`
- `uudemon.admin`
- `uudemon.cleanup`

Diese Skripten sollten regelmäßig ausgeführt werden, um sicherzustellen, dass UUCP reibungslos funktioniert. Die zum Ausführen der Skripten dienende `crontab`-Datei wird automatisch in `/usr/lib/uucp/uudemon.crontab` als Teil des Solaris-Installationsprozesses erstellt, wenn Sie die vollständige Installation wählen. Ansonsten wird die Datei erstellt, wenn Sie das UUCP-Paket installieren.

Sie können die UUCP-Shell-Skripten auch manuell ausführen. Es folgt die `uudemon.crontab`-Prototypdatei, die Sie für einen bestimmten Rechner anpassen können:

```
#
#ident  "@(#)uudemon.crontab    1.5     97/12/09 SMI"
#
# This crontab is provided as a sample. For systems
# running UUCP edit the time schedule to suit, uncomment
# the following lines, and use crontab(1) to activate the
# new schedule.
#
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin
#20 3 * * * /usr/lib/uucp/uudemon.cleanup
#0 * * * * /usr/lib/uucp/uudemon.poll
#11,41 * * * * /usr/lib/uucp/uudemon.hour
```

Hinweis – UUCP-Vorgänge sind standardmäßig deaktiviert. Um UUCP zu aktivieren, bearbeiten Sie den Zeitplan und entfernen Kommentare aus den entsprechenden Zeilen in der `uudemon.crontab` -Datei .

▼ So starten Sie UUCP

Gehen Sie wie folgt vor, um die `uudemon.crontab`-Datei zu aktivieren:

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Bearbeiten Sie die `/usr/lib/uucp/uudemon.crontab` -Datei, und ändern Sie nach Bedarf die Einträge.**

3. **Aktivieren Sie die `uudemon.crontab`-Datei, indem Sie den folgenden Befehl ausgeben:**

   ```
   crontab < /usr/lib/uucp/uudemon.crontab
   ```

`uudemon.poll`-Shell-Skript

Das standardmäßige `uudemon.poll`-Shell-Skript liest einmal pro Stunde die `/etc/uucp/Poll`-Datei. Wenn geplant ist, dass die in der `Poll`-Datei angegebenen Rechner abgefragt werden sollen, wird eine Arbeitsdatei (`C.`*sysnxxxx*) im `/var/spool/uucp/`*nodename*-Verzeichnis abgelegt. *nodename* stellt den UUCP-Knotennamen des Rechners dar.

Das Shell-Skript wird wie geplant einmal pro Stunde vor `uudemon.hour` ausgeführt, sodass die Arbeitsdateien im Verzeichnis abgelegt sind, wenn `uudemon.hour` aufgerufen wird.

`uudemon.hour`-Shell-Skript

Das standardmäßige `uudemon.hour`-Shell-Skript führt folgende Vorgänge aus:

- Aufrufen des `uusched`-Programms zum Durchsuchen der Spool-Verzeichnisse nach Arbeitsdateien (`C.`), die noch nicht verarbeitet wurden. Anschließend plant das Skript die Übertragung dieser Dateien an einen Remote-Rechner.
- Aufrufen des `uuxqt`-Dämons zum Durchsuchen der Spool-Verzeichnisse nach Ausführungsdateien (`X.`), die an Ihren Rechner übertragen wurden und während dieses Vorgangs nicht verarbeitet wurden

`uudemon.hour` wird standardmäßig zweimal pro System ausgeführt. Sie können `uudemon.hour` häufiger ausführen, wenn Sie hohe Fehlerquoten der Aufrufe erwarten, die an Remote-Rechner gesendet werden.

uudemon.admin-Shell-Skript

Das standardmäßige uudemon.admin-Shell-Skript führt folgende Vorgänge aus:

- Ausführen des Befehls uustat in Verbindung mit den Optionen p und q. Mithilfe der Option q wird der Status der Arbeitsdateien (C.), der Datendateien (D.) und der Ausführungsdateien (X.) gemeldet, die sich in der Warteschlange befinden. Mithilfe der Option p werden Prozessinformationen für Vernetzungsprozesse ausgegeben, die in den Sperrdateien (/var/spool/locks) aufgelistet sind.
- Senden von Statusinformationen an die uucp-Verwaltungsanmeldung mithilfe von mail

uudemon.cleanup-Shell-Skript

Die standardmäßige uudemon.cleanup-Shell-Skript führt folgende Vorgänge aus:

- Sammeln von Protokolldateien für bestimmte Rechner aus dem /var/uucp/.Log-Verzeichnis, Zusammenführen dieser Dateien und Ablegen dieser Dateien im /var/uucp/.Old-Verzeichnis zusammen mit anderen älteren Protokollinformationen
- Entfernen von Arbeitsdateien (C.), die sieben Tage alt oder älter sind, Datendateien (D.), die sieben Tage oder älter sind, und Ausführungsdateien (X.), die zwei Tage oder älter sind, aus den Spool-Dateien
- Gibt nicht zustellbare Mails an den Absender zurück
- Senden einer Zusammenfassung der Statusinformationen, die im Laufe des aktuellen Tags für die UUCP-Verwaltungsanmeldung (uucp) gesammelt wurden

Ausführen von UUCP über TCP/IP

Um UUCP über ein TCP/IP-Netzwerk auszuführen, müssen einige Modifizierungen vorgenommen werden, was in diesem Abschnitt beschrieben wird.

▼ So aktivieren Sie UUCP für TCP/IP

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Bearbeiten Sie die /etc/uucp/Systems -Datei, um sicherzustellen, dass die Einträge folgende Felder aufweisen:**

Systemname Zeit TCP-Port Netzwerkname Standard-Anmelde-Chat

Ein typischer Eintrag hat folgendes Aussehen:

```
rochester Any TCP - ur-seneca login: Umachine password: xxx
```

Beachten Sie, dass das Feld *Netzwerkname* Ihnen erlaubt, explizit den TCP/IP-Hostnamen anzugeben. Diese Fähigkeit ist für manche Standorten wichtig. Im vorangegangenen Beispiel hat der Standort den UUCP-Knotennamen `rochester` , der sich von seinem TCP/IP-Hostnamen `ur-seneca` unterscheidet. Außerdem kann ein völlig anderer Rechner problemlos UUCP ausführen und den TCP/IP-Hostnamen von `rochester` verwenden.

Das Feld "Port" in der `Systems`-Datei sollte den Eintrag `-` aufweisen. Diese Syntax entspricht der Auflistung des Eintrags als `uucp`. In fast jeder Situation entspricht der *Netzwerkname* dem Systemnamen, und das Feld "Port" ist `-`, was bedeutet, dass der standardmäßige UUCP-Port aus der `Services`-Datenbank verwendet wird. Der `in.uucpd`-Dämon erwartet, dass der Remote-Rechner seine Anmeldung und sein Passwort für die Authentifizierung sendet. `in.uucpd` fordert diese Informationen ebenso wie `getty` und `login` an.

3 Bearbeiten Sie die `/etc/inet/services`-Datei, um einen Port für UUCP einzurichten:

```
uucp    540/tcp    uucpd        # uucp daemon
```

Der Eintrag muss normalerweise nicht geändert werden. Wenn Ihr Rechner jedoch NIS oder NIS+ als Name Service ausführt, sollten Sie den `/etc/nsswitch.conf`-Eintrag für `/etc/services` ändern, um zunächst `files` und dann `nis` oder `nisplus` zu überprüfen.

4 Stellen Sie sicher, dass UUCP aktiviert ist.

```
# svcs network/uucp
```

Der UUCP-Service wird durch die Service Management Facility verwaltet. Um den Status dieses Service abzufragen, können Sie den Befehl `svcs` verwenden. Eine Übersicht zur Service Management Facility finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*.

5 (Optional) Aktivieren Sie UUCP nach Bedarf, indem Sie Folgendes eingeben:

```
# inetadm -e network/uucp
```

UUCP-Sicherheit und Verwaltung

Nachdem Sie UUCP eingerichtet haben, gestaltet sich die Verwaltung recht einfach. In diesem Abschnitt werden laufende UUCP-Aufgaben erläutert, die im Zusammenhang mit der Sicherheit, Verwaltung und Fehlerbehebung stehen.

Einrichten der UUCP-Sicherheit

Die standardmäßige `/etc/uucp/Permissions` -Datei bietet maximale Sicherheit für Ihre UUCP-Verbindungen. Die standardmäßige `Permissions`-Dateien enthält keine Einträge.

Sie können zusätzliche Parameter für jedem Remote-Rechner festlegen, um Folgendes zu definieren:

- die Art und Weise, wie der Remote-Rechner Dateien von Ihrem Rechner empfangen kann
- Verzeichnisse, für die der Remote-Rechner über Lese- und Schreibzugriff verfügt
- Befehle, die der Remote-Rechner verwenden kann, um Remote-Vorgänge auszuführen

Es folgt eine typischer Berechtigungseintrag:

```
MACHINE=datsun LOGNAME=Udatsun VALIDATE=datsun
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

Dieser Eintrag erlaubt, dass Dateien an "normale" UUCP-Verzeichnissen gesendet und von diesen empfangen werden können, nicht aber von anderen Stellen im System. Außerdem bewirkt der Eintrag, dass der UUCP-Benutzername zum Zeitpunkt der Anmeldung geprüft wird.

Reguläre UUCP-Verwaltung

UUCP erfordert nur wenig Verwaltungsaufwand. Sie müssen jedoch sicherstellen, dass die `crontab`-Datei vorhanden ist (siehe Abschnitt „So starten Sie UUCP“ auf Seite 588). Ihr Augenmerk sollte auf die Zunahme der Anzahl von Maildateien und der Größe des öffentlichen Verzeichnisses gerichtet sein.

E-Mail für UUCP

Alle E-Mail-Nachrichten, die von den UUCP-Programmen und Skripten generiert werden, werden an das Benutzer-ID-`uucp` gesendet. Wenn Sie sich weniger häufig als der betreffende Benutzer anmelden, werden Sie eventuell nicht bemerken, dass sich Mails ansammeln und Festplattenspeicher belegen. Um dieses Problem zu lösen, erstellen Sie ein Alias in `/etc/mail/aliases` und leiten diese E-Mails entweder direkt an `root` oder an sich selbst und andere um, die für die Verwaltung von UUCP verantwortlich sind. Vergessen Sie nicht, den Befehl `newaliases` auszuführen, nachdem Sie die `aliases`-Datei modifiziert haben.

Öffentliches UUCP-Verzeichnis

Das in jedem System vorhandene Verzeichnis `/var/spool/uucppublic` ist ein Speicherort, in den UUCP standardmäßig Dateien kopieren kann. Jeder Benutzer ist berechtigt, Änderungen an `/var/spool/uucppublic` vorzunehmen und Dateien, die sich in diesem Verzeichnis befinden, zu lesen und zu beschreiben. Da jedoch das Sticky-Bit gesetzt ist, ist der Modus des Verzeichnisses 01777. Dadurch können Benutzer keine Dateien entfernen, die in das Verzeichnis kopiert wurden und zu `uucp` gehören. Nur Sie können Dateien aus diesem Verzeichnis entfernen, sofern Sie als `root`- oder `uucp`-Benutzer angemeldet sind. Um eine unkontrollierte Ansammlung von Dateien in diesem Verzeichnis zu vermeiden, sollte sichergestellt sein, dass die Dateien regelmäßig aus dem Verzeichnis entfernt werden.

Wenn diese Art der Verwaltung für die Benutzer unpraktisch ist, können Sie ihnen empfehlen, `uuto` und `uupick` zu verwenden, anstatt das Sticky-Bit zu entfernen, das aus Sicherheitsgründen gesetzt ist. Auf der Manpage `uuto(1C)` finden Sie Informationen zur Verwendung von `uuto` und `uupick`. Auch können Sie den Modus des Verzeichnisses auf eine Gruppe von Benutzern beschränken. Wenn Sie nicht riskieren wollen, dass jemand Ihre Festplatte belegt, können Sie sogar den UUCP-Zugriff auf die Festplatte verhindern.

UUCP-Fehlerbehebung

Anhand dieser Verfahren können Sie allgemeine UUCP-Probleme beheben.

▼ So stellen Sie fest, ob fehlerhafte Modems oder ACUs vorhanden sind

Es gibt mehrere Möglichkeiten, um festzustellen, ob Modems oder andere ACUs nicht richtig funktionieren.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Mithilfe des folgenden Befehls können Sie Zählungen und Ursachen für Verbindungsausfälle abrufen:**

   ```
   # uustat -q
   ```

3. **Führen Sie eine Anwahl über eine bestimmte Verbindung aus, und rufen Sie eine Ausgabe der Fehlerbehebungsinformationen ab, die diesen Versuch betreffen.**

   Die Zeile muss in der `/etc/uucp/Devices`-Datei mit `direct` definiert sein. Sie müssen am Ende der Befehlszeile eine Telefonnummer eintragen, wenn die Leitung mit einer automatischen Wähleinrichtung verbunden ist oder das Gerät mit `direct` eingerichtet werden muss. Geben Sie Folgendes ein:

   ```
   # cu -d -l line
   ```

   line ist `/dev/cua/a`.

▼ So suchen Sie Übertragungsfehler

Wenn Sie keine Verbindung mit einem bestimmten Rechner aufnehmen können, können Sie die Kommunikation mit dem Rechner mithilfe von `Uutry` und `uucp` prüfen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Versuchen Sie, Kontakt herzustellen:**

   ```
   # /usr/lib/uucp/Uutry -r machine
   ```

   Ersetzen Sie *Rechner* durch den Hostnamen des Rechners, mit dem Sie keinen Kontakt aufnehmen können. Dieser Befehl:

   - Startet den Übertragungsdämon (`uucico`) einschließlich der Fehlersuche. Weitere Informationen zur Fehlersuche erhalten Sie, wenn Sie sich als Root-Benutzer anmelden.
   - Leitet die Ausgabe der Fehlersuche an `/tmp/` *Rechner* weiter.
   - Gibt die Ausgabe der Fehlersuche an Ihr Terminal weiter, indem der folgende Befehl ausgegeben wird:

     ```
     # tail -f
     ```

     Drücken Sie Strg+C, um die Ausgabe zu beenden. Sie können die Ausgabe von `/tmp/` *Rechner* kopieren, um die Ausgabe zu speichern.

3. **Wenn das Problem nicht mit `Uutry` eingegrenzt werden kann, versuchen Sie, einen Job in die Warteschlange zu stellen:**

   ```
   # uucp -r file machine\!/dir/file
   ```

Datei	Verwenden Sie den Namen der Datei, die übertragen werden soll.
Rechner	Verwenden Sie den Namen des Rechners, auf den kopiert werden soll.
/Verzeichnis/Datei	Geben Sie den Speicherort der Datei für den anderen Rechner an.

4. **Geben Sie den folgenden Befehl aus:**

   ```
   # Uutry
   ```

   Wenn das Problem dadurch immer noch nicht behoben werden kann, wenden Sie sich an den lokalen Mitarbeiter, der für technische Unterstützung zuständig ist. Speichern Sie die Ausgabe der Fehlersuche, die bei der Diagnostizierung des Problems hilfreich sein kann.

Hinweis – Auch können Sie die von `Uutry` bereitgestellte Fehlersuchebene mithilfe der Option `-x` *n* herabsetzen oder erhöhen. *n* zeigt die Fehlersuchebene an. Die standardmäßige Fehlersuchebene für `Uutry` ist 5.

Die Fehlersuchebene 3 stellt grundlegende Informationen zum Zeitpunkt und zur Art und Weise der Herstellung der Verbindung bereit. Es werden jedoch nur wenige Informationen zur Übertragung bereitgestellt. Die Fehlersuchebene 9 hingegen bietet umfassende Informationen zur zur Übertragung. Beachten Sie, dass die Fehlersuche an beiden Enden der Übertragungsverbindung stattfindet. Wenn Sie vorhaben, eine höhere als die Fehlersuchebene 5 bei einem moderat großen Text zu verwenden, kontaktieren Sie den Administrator am anderen Ende, um festzustellen, wann die Ebene geändert werden muss.

Prüfen der UUCP-`/etc/uucp/Systems`-Datei

Stellen Sie sicher, dass die Informationen in Ihrer `Systems`-Datei auf dem neuesten Stand sind, wenn Sie Mühe haben, einen bestimmten Rechner zu kontaktieren. Folgende rechnerbezogene Informationen können nicht auf dem neuesten Stand sein:

- Telefonnummer
- Anmelde-ID
- Passwort

Prüfen von UUCP-Fehlermeldungen

UUCP hat zwei Typen von Fehlermeldungen: `ASSERT` und `STATUS`.

- Wenn ein Prozess abgebrochen wird, werden `ASSERT`-Fehlermeldungen in `/var/uucp/.Admin/errors` gespeichert. In diesen Meldungen ist der Dateiname, `sccsid`, die Zeilennummer und Text enthalten. Diese Meldungen resultieren normalerweise aus Systemproblemen.
- `STATUS`-Fehlermeldungen werden im `/var/uucp/.Status`-Verzeichnis gespeichert. Das Verzeichnis enthält eine separate Datei für jeden Remote-Rechner, mit dem Ihr Rechner zu kommunizieren versucht. Diese Dateien enthalten Statusinformationen zu den Kommunikationsversuchen und darüber, ob diese Versuche Erfolg hatten.

Prüfen von grundlegenden Informationen

Es stehen mehrere Befehle zum Prüfen von grundlegenden Vernetzungsinformationen zur Verfügung:

- Verwenden Sie den Befehl `uuname`, um die Rechner aufzulisten, die Ihr Rechner kontaktieren kann.
- Verwenden Sie den Befehl `uulog`, um den Inhalt der Protokollverzeichnisse für bestimmte Hosts anzuzeigen.
- Verwenden Sie den Befehl `uucheck -v`, um festzustellen, ob die Dateien und Verzeichnisse vorhanden sind, die von `uucp` benötigt werden. Zudem ermöglicht dieser Befehl, die `Permissions`-Datei zu prüfen und Informationen zu den von Ihnen eingerichteten Berechtigungen anzuzeigen.

◆ ◆ ◆ KAPITEL 26

UUCP (Referenz)

Dieses Kapitel enthält Referenzinformationen für das Arbeiten mit UUCP. Folgende Themen werden behandelt:

- „/etc/uucp/Systems-UUCP-Datei“ auf Seite 597
- „ /etc/uucp/Devices-UUCP-Datei“ auf Seite 605
- „ /etc/uucp/Dialers-UUCP-Datei“ auf Seite 612
- „Weitere grundlegende UUCP-Konfigurationsdateien“ auf Seite 616
- „ /etc/uucp/Permissions-UUCP-Datei“ auf Seite 619
- „UUCP- /etc/uucp/Poll-Datei“ auf Seite 628
- „UUCP- /etc/uucp/Config-Datei“ auf Seite 628
- „UUCP- /etc/uucp/Grades-Datei“ auf Seite 628
- „Weitere UUCP-Konfigurationsdateien“ auf Seite 631
- „UUCP-Verwaltungsdateien“ auf Seite 633
- „UUCP-Fehlermeldungen“ auf Seite 635

/etc/uucp/Systems-UUCP-Datei

Die /etc/uucp/Systems -Datei enthält Informationen, die der uucico-Dämon benötigt, um eine Kommunikationsverbindung mit einem Remote-Computer herzustellen. /etc/uucp/Systems ist die erste Datei, die Sie benötigen, um UUCP zu bearbeiten.

Jeder Eintrag in der Systems -Datei stellt einen Remote-Computer dar, mit dem Ihr Host kommuniziert. Ein Host kann mehrere Einträge haben. Die zusätzlichen Einträge stellen Kommunikationspfade dar, die nacheinander verwendet werden. Außerdem wird durch UUCP standardmäßig verhindert, dass ein Computer, der nicht in /etc/uucp/Systems angegeben ist, sich bei Ihrem Host anmeldet.

Mithilfe der Sysfiles -Datei können Sie mehrere Dateien definieren, die als Systems-Dateien verwendet werden sollen. Unter „ /etc/uucp/Sysfiles-UUCP-Datei “ auf Seite 617 finden Sie eine Beschreibung von Sysfiles.

Es folgt die Syntax eines Eintrags in der `Systems`-Datei:

```
System-Name    Time    Type    Speed    Phone    Chat Script
```

Nachstehend wird ein Beispiel für einen Eintrag in der `Systems`-Datei gezeigt.

BEISPIEL 26–1 Eintrag in `/etc/uucp/Systems`

```
Arabian     Any  ACUEC 38400 111222  ogin: Puucp ssword:beledi
```

`Arabian`	Eintrag für das Feld "System-Name". Weitere Informationen finden Sie unter „Feld "System-Name" in der `/etc/uucp/Systems`-Datei“ auf Seite 598.
`Any`	Eintrag für das Feld "Time". Weitere Informationen finden Sie unter „Feld "Time" in `/etc/uucp/Systems`-Datei“ auf Seite 599.
`ACUEC`	Eintrag für das Feld "Type". Weitere Informationen finden Sie unter „Feld "Type" in `/etc/uucp/Systems`-Datei“ auf Seite 600.
`38400`	Eintrag für das Feld "Speed". Weitere Informationen finden Sie unter „Feld "Speed" in `/etc/uucp/Systems`-Datei“ auf Seite 600.
`111222`	Eintrag für das Feld "Phone". Weitere Informationen finden Sie unter „Feld "Phone" in `/etc/uucp/Systems`-Datei“ auf Seite 601.
`ogin: Puucp ssword:beledi`	Eintrag für das Feld "Chat Script". Weitere Informationen finden Sie unter „Feld "Chapt Script" in `/etc/uucp/Systems`-Datei“ auf Seite 601.

Feld "System-Name" in der `/etc/uucp/Systems`-Datei

Dieses Feld enthält den Knotennamen des Remote-Computers. In TCP/IP-Netzwerken kann dieser Name der Hostname eines Rechners oder ein Name sein, der eigens für die UUCP-Kommunikation durch die `/etc/uucp/Sysname` -Datei erstellt wird. Lesen Sie dazu „`/etc/uucp/Systems`-UUCP-Datei“ auf Seite 597. In Beispiel 26–1 enthält das Feld "System-Name" einen Eintrag für den Remote-Host `Arabian` .

Feld "Time" in `/etc/uucp/Systems`-Datei

In diesem Feld wird anhand des Wochentags und der Uhrzeit angegeben, wann der Remote-Computer aufgerufen werden kann. Das Feld "Time" hat das folgende Format:

```
daytime[;retry]
```

Teil "*day*" des Felds "Time"

Der Teil "*day*" kann eine Liste sein, die einige der folgenden Einträge enthält:

`Su Mo Tu We Th Fr Sa`	für bestimmte Tage.
`Wk`	für einen Wochentag.
`Any`	für einen beliebigen Tag.
`Never`	Ihr Host initiiert nie einen Aufruf eines Remote-Computers. Der Aufruf muss vom Remote-Computer initiiert werden. Ihr Host wird dann im *passiven Modus* ausgeführt.

Teil "*time*" des Felds "Time"

Beispiel 26–1 zeigt den Eintrag `Any` im Feld "Time". Dieser Eintrag zeigt an, dass der Host `Arabian` jederzeit aufgerufen werden kann.

Der Teil "*time*" dient zur Angaben von Zeiten im 24-Stunden-Format. `0800-1230` steht beispielsweise für 8:30 Uhr bis 12:30 Uhr. Wenn der Teil "*time*" nicht angegeben ist, kann ein Aufruf zu jeder beliebigen Tageszeit durchgeführt werden.

Ein Zeitbereich, der 0000 umfasst, ist zugelassen. `0800-0600` bedeutet beispielsweise, dass alle Uhrzeiten außer den Uhrzeiten zwischen 6 und 8 Uhr vormittags zugelassen sind.

Teil "*retry*" des Felds "Time"

Anhand des Unterfelds "*retry*" können Sie die Mindestzeit (in Minuten) angeben, die verstreichen muss, bevor nach einem fehlgeschlagenen Versuch ein erneuter Versuch ausgeführt wird. Die standardmäßige Wartezeit beträgt 60 Minuten. Das Trennzeichen des Unterfelds ist ein Semikolon (;). `Any;9` wird beispielsweise als Aufruf aufgefasst, der jederzeit erfolgen kann. Allerdings muss nach einem fehlgeschlagenen Aufruf mindestens 9 Minuten gewartet werden, eher ein weiterer Versuch unternommen werden kann.

Wenn Sie keinen Eintrag "*retry*" angeben, wird ein exponentieller Verzögerungsalgorithmus verwendet. Das bedeutet, dass UUCP mit einer standardmäßigen Wartezeit beginnt, die mit jedem fehlgeschlagenen Versuch verlängert wird. Die anfängliche Wiederholungszeit zwischen den Versuchen beträgt beispielsweise 5 Minuten. Wenn ein Versuch erfolglos bleibt, wird der

nächste Versuch 10 Minuten später durchgeführt. Bleibt auch dieser Versuch erfolglos, wird der nächste Versuch 20 Minuten später durchgeführt usw., bis die maximale Zeit von 23 Stunden erreicht ist. Wenn "*retry*" angegeben ist, entspricht der angegebene Wert immer der Wiederholungszeit. Anderenfalls wird der Verzögerungalgorithmus verwendet.

Feld "Type" in `/etc/uucp/Systems`-Datei

Dieses Feld enthält den Gerätetyp, der verwendet wird, um die Kommunikationsverbindung mit dem Remote-Computer herzustellen. Das in diesem Feld verwendete Schlüsselwort wird mit dem ersten Feld der `Devices`-Dateieinträge abgeglichen.

BEISPIEL 26–2 Schlüsselwort für das Feld "Type"

```
Arabian    Any    ACUEC, g    38400    1112222    ogin: Puucp ssword:beledi
```

Sie können das Protokoll definieren, das zum Kontaktieren des Systems verwendet wird, indem Sie das Protokoll in das Feld "Type" einfügen. Das vorangegangene Beispiel zeigt, wie das Protokoll `g` dem Gerätetyp `ACUEC` zugeordnet wird. Weitere Informationen zu Protokollen finden Sie unter „Protokolldefinitionen in `/etc/uucp/Devices`-Datei“ auf Seite 611.

Feld "Speed" in `/etc/uucp/Systems`-Datei

Dieses Feld, das auch als Feld "Class" bezeichnet wird, dient zur Angabe der Übertragungsgeschwindigkeit des Geräts, das zum Herstellen der Kommunikationsverbindung verwendet wird. Das UUCP-Feld "Speed" kann einen Buchstaben und die Geschwindigkeit (beispielsweise `C1200` oder `D1200`) enthalten, damit zwischen den Klassen der Dialer unterschieden werden kann. Lesen Sie dazu „Feld "Class" in `/etc/uucp/Devices`-Datei“ auf Seite 607.

Bei manchen Geräten kann jede Geschwindigkeit verwendet werden. Geben Sie dann das Schlüsselwort `Any` an. Dieses Feld muss mit dem Feld "Class" im entsprechenden `Devices`-Dateieintrag übereinstimmen.

BEISPIEL 26–3 Eintrag im Feld "Speed"

```
eagle    Any    ACU, g    D1200    NY3251    ogin: nuucp ssword:Oakgrass
```

Wenn für dieses Feld keine Informationen erforderlich sind, verwenden Sie einen Bindestrich (-) als Platzhalter.

Feld "Phone" in /etc/uucp/Systems-Datei

Dieses Feld ermöglicht Ihnen, die auch als *Token* bezeichnete Telefonnummer des Remote-Computers für automatische Dialer anzugeben, die als *Portselektoren* bezeichnet werden. Die Telefonnummer besteht aus einem optionalen alphabetischen Kürzel und einem numerischen Teil. Wenn ein Kürzel verwendet wird, muss es in der `Dialcodes` -Datei aufgelistet sein.

BEISPIEL 26–4 Eintrag im Feld "Phone"

```
nubian     Any    ACU       2400    NY555-1212    ogin: Puucp ssword:Passuan
eagle      Any    ACU, g    D1200   NY=3251       ogin: nuucp ssword:Oakgrass
```

Ein Gleichheitszeichen (`=`) im Feld `Phone` bewirkt, dass die `ACU` auf einen zweiten Wählton wartet, bevor die übrigen Ziffern gewählt werden. Ein Bindestrich (`-`) in der Zeichenfolge bewirkt, dass die `ACU` vier Sekunden wartet, bevor die nächste Ziffer gewählt wird.

Wenn Ihr Computer mit einem Portselektor verbunden ist, können Sie auf andere Computer zugreifen, die mit diesem Selektor verbunden sind. Die `Systems`-Dateieinträge für diese Remote-Rechner dürfen keine Telefonnummer im Feld `Phone` aufweisen. Stattdessen muss in diesem Feld das Token enthalten sein, dass an den Switch weitergegeben wird. Dadurch ist dem Portselektor der Remote-Rechner bekannt, mit dem Ihr Host kommunizieren soll. Normalerweise ist dies einfach der Systemname. Am Ende des zugehörigen `Devices`-Dateieintrags muss `\D` stehen, um sicherzustellen, dass dieses Feld nicht mithilfe der `Dialcodes`-Datei übersetzt wird.

Feld "Chapt Script" in /etc/uucp/Systems-Datei

Dieses Feld, das auch als Anmeldefeld bezeichnet wird, enthält eine Zeichenfolge, die als *Chat-Skript* bezeichnet wird. Das Chat-Skript enthält die Zeichen, die die lokalen und Remote-Rechner während des Anfangsdialogs austauschen müssen. Chat-Skripten haben folgendes Format:

expect send [expect send] ....

expect stellt eine Zeichenfolge dar, die der lokale Host vom Remote-Host erwartet, damit der Dialog eingeleitet werden kann. *send* ist die Zeichenfolge, die vom lokalen Host gesendet wird, nachdem er die Zeichenfolge *expect* vom Remote-Host erhalten hat. Ein Chat-Skript kann mehrere expect-send-Sequenzen haben.

Ein grundlegendes Chat-Skript kann Folgendes enthalten:

- Eine Anmeldeaufforderung, die der lokale Host vom Remote-Rechner erwartet
- Ein Anmeldename, den der lokale Host an den Remote-Rechner sendet, um sich anzumelden
- Eine Aufforderung zur Passworteingabe, die der lokale Host vom Remote-Rechner erwartet
- Ein Passwort, das der lokale Host an den Remote-Rechner sendet

Das Feld "*expect*" kann aus Unterfeldern bestehen, die folgende Form haben:

expect[-send-expect]...

-send wird gesendet, wenn *expect* nicht erfolgreich gelesen werden kann. Das Unterfeld *-expect*, das dem Unterfeld *-send* folgt, ist die nächste erwartete Zeichenfolge.

Bei den Zeichenfolgen `login--login` erwartet das UUCP auf dem lokalen Host die Zeichenfolge `login`. Wenn das UUCP die Zeichenfolge `login` vom Remote-Rechner empfängt, fährt das UUCP mit dem nächsten Feld fort. Wenn das UUCP nicht die Zeichenfolge `login` empfängt, sendet das UUCP ein Wagenrücklaufzeichen und sucht dann erneut nach `login`. Wenn der lokale Computer anfangs keine Zeichen erwartet, verwenden Sie im Feld *expect* die Zeichen "" (für eine Null-Zeichenfolge). Alle *send* -Felder werden mit einem nachgestellten Wagenrücklaufzeichen gesendet, es sei denn, die *send*-Zeichenfolge endet mit `\c`.

Es folgt ein Beispiel eines `Systems`-Dateieintrags, in dem eine *expect-send* -Zeichenfolge verwendet wird:

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzzy
```

In diesem Beispiel wird das UUCP auf dem lokalen Host angewiesen, zwei Wagenrücklaufzeichen zu senden und auf `ogin:` (für `Login:`) zu warten. Wenn `ogin`: nicht empfangen wird, senden Sie ein `BREAK`. Wenn Sie `ogin:` empfangen, senden Sie den Anmeldenamen `Puucpx`. Wenn Sie `ssword:` (für `Password:`) empfangen, senden Sie das Passwort `xyzzy`.

In der nachstehenden Tabelle sind einige nützliche Escape-Zeichen aufgelistet.

TABELLE 26–1 Escape-Zeichen, die im Feld "Chat-Script" der `Systems` -Datei verwendet werden

Escape-Zeichen	Bedeutung
`\b`	Sendet oder erwartet ein Rückschrittzeichen.
`\c`	Wenn dieses Escape-Zeichen am Ende einer Zeichenfolge steht, unterdrückt es das Wagenrücklaufzeichen, das normalerweise gesendet wird. Anderenfalls wird dieses Escape-Zeichen ignoriert.

TABELLE 26–1 Escape-Zeichen, die im Feld "Chat-Script" der `Systems` -Datei verwendet werden *(Fortsetzung)*

Escape-Zeichen	Bedeutung
`\d`	Bewirkt eine Verzögerung um 1 bis 3 Sekunden, bevor weitere Zeichen gesendet werden.
`\E`	Startet die Echoprüfung. Wenn von diesem Punkt an ein Zeichen übertragen wird, wartet das UUCP auf den Empfang des Zeichens, bevor es mit der Prüfung fortfährt.
`\e`	Deaktiviert die Echoprüfung.
`\H`	Ignoriert ein Aufhängen. Verwenden Sie diese Option für Rückrufmodems.
`\K`	Sendet ein BREAK-Zeichen.
`\M`	Aktiviert das `CLOCAL`-Flag.
`\m`	Deaktiviert das `CLOCAL`-Flag.
`\n`	Sendet oder erwartet ein Zeilenvorschubzeichen.
`\N`	Sendet ein NULL-Zeichen (ASCII NUL).
`\p`	Wartet etwa eine viertel bis eine halbe Sekunde.
`\r`	Sendet oder erwartet ein Wagenrücklaufzeichen.
`\s`	Sendet oder erwartet ein Leerzeichen.
`\t`	Sendet oder erwartet ein Tabulatorzeichen.
`EOT`	Sendet ein EOT, gefolgt von zwei Zeilenvorschubzeichen.
`BREAK`	Sendet ein BREAK-Zeichen.
`\`*ddd*	Sendet oder erwartet das Zeichen, das durch die Oktalziffern (*ddd*) dargestellt wird.

Aktivieren des Rückrufs durch das Chat-Skript

Manche Unternehmen setzen Einwahlserver zur Verarbeitung der Aufrufe von Remote-Computern ein. Ihr Unternehmen könnte beispielsweise einen Einwahlserver mit einem Einwahlmodem haben, das Mitarbeiter von ihren Heimcomputern aus aufrufen können. Nachdem der Einwahlserver den Remote-Rechner identifiziert hat, trennt er die bestehende Verbindung und ruft den Remote-Rechner dann zurück. Dann wird die Kommunikationsverbindung wiederhergestellt.

Sie können den Rückruf vereinfachen, indem Sie die Option `\H` im Chat-Skript der `Systems`-Datei an der Stelle einfügen, an der der Rückruf durchgeführt werden soll. Fügen Sie `\H` als Teil einer expect-Zeichenfolge an der Stelle ein, an der der Einwahlserver voraussichtlich "auflegt".

Angenommen, das Chat-Skript, das den Einwahlserver aufruft, enthält die folgende Zeichenfolge:

```
INITIATED\Hogin:
```

Die UUCP-Wähleinrichtung auf dem lokalen Rechner erwartet den Empfang der Zeichen (`INITIATED`) vom Einwahlserver. Nachdem die Zeichen (`INITIATED`) abgeglichen wurden, entfernt die Wähleinrichtung alle nachfolgenden Zeichen, die von ihr empfangen werden, bis der Einwahlserver "auflegt". Die lokale Wähleinrichtung wartet, bis sie den nächsten Teil der erwarteten Zeichenfolge, die Zeichen `ogin:`, vom Einwahlserver empfängt. Sobald die Wähleinrichtung die Zeichen `ogin:` empfangen hat, fährt sie mit dem Durchlaufen des Chat-Skripts fort.

Eine Zeichenfolge muss dem Zeichen `\H` nicht direkt vorangestellt oder nachgestellt sein, wie in der vorangegangenen Beispielzeichenfolge zu sehen ist.

Hardware-Flusskontrolle in `/etc/uucp/Systems` -Datei

Sie können auch die `STTY=`*value*-Pseudo-Sendezeichenfolge verwenden, um die Modemeigenschaften zu definieren. Die Hardware-Flusskontrolle kann beispielsweise mit `STTY=crtscts` aktiviert werden. `STTY` akzeptiert alle `stty`-Modi. Ausführliche Informationen finden Sie auf den Manpages `stty(1)` und `termio(7I)`.

Im folgenden Beispiel wird die Hardware-Flusskontrolle in einem `Systems` -Dateieintrag aktiviert:

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtscts
```

Diese Pseudo-Sendezeichenfolge kann auch in den Einträgen in der `Dialers`-Datei verwendet werden.

Einstellen der Parität in `/etc/uucp/Systems`-Datei

In manchen Fällen müssen Sie die Parität zurücksetzen, weil das System, das Sie aufrufen, die Portparität prüft und die Verbindung unterbricht, wenn die Parität falsch ist. Das expect-send-Paar, "" `P_ZERO`, setzt das hochwertige Bit (Paritätsbit) auf 0. Beachten Sie das expect-send-Paar im folgenden Beispiel:

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

Es folgen Paritätspaare, die dem expect-send-Paar, "" `P_ZERO`, nachgestellt sein können:

"" `P_EVEN` Setzt die Parität auf gerade Werte (Standardeinstellung).

"" P_ODD Setzt die Parität auf ungerade Werte.

"" P_ONE Setzt das Paritätsbit auf 1.

Diese Paritätspaare können überall im Chat-Skript eingefügt werden. Die Paritätspaare haben für alle Informationen im Chat-Skript Gültigkeit, die nach "" P_ZERO, dem expect-send-Paar, folgen. Ein Paritätspaar kann auch in den Einträgen in der Dialers-Datei verwendet werden. Im folgenden Beispiel ist das Paritätspaar "" P_ONE enthalten:

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

/etc/uucp/Devices-UUCP-Datei

Die /etc/uucp/Devices -Datei enthält Informationen für alle Geräte, die verwendet werden können, um eine Verbindung mit einem Remote-Computer herzustellen. Bei diesen Geräten und Einrichtungen handelt es sich um ACUs (einschließlich Hochgeschwindigkeitsmodems), direkte Verbindungen und Netzwerkverbindungen.

Ein Eintrag in der /etc/uucp/Devices -Datei hat folgende Syntax:

```
Type   Line   Line2   Class   Dialer-Token-Pairs
```

Es folgt ein Eintrag in der Devices-Datei für ein U.S. Robotics V.32bis-Modem, das an Port A angeschlossen ist und mit einer Übertragungsgeschwindigkeit von 38.400 Bit/s läuft.

```
ACUEC   cua/a   -   38400   usrv32bis-ec
```

ACUEC Eintrag im Feld "Type". Weitere Informationen finden Sie unter „Feld "Type" in /etc/uucp/Devices-Datei“ auf Seite 606.

cua/a Eintrag im Feld "Line". Weitere Informationen finden Sie unter „Feld "Line" in /etc/uucp/Devices-Datei“ auf Seite 607.

- Eintrag im Feld "Line2". Weitere Informationen finden Sie unter „Feld "Line2" in /etc/uucp/Devices-Datei“ auf Seite 607.

38400 Eintrag im Feld "Class". Weitere Informationen finden Sie unter „Feld "Class" in /etc/uucp/Devices-Datei“ auf Seite 607.

usrv32bis-ec Eintrag im Feld "Dialer-Token-Pairs" (DTP). Weitere Informationen finden Sie unter „Feld "Dialer-Token-Pairs" in /etc/uucp/Devices-Datei“ auf Seite 608.

Alle Felder werden im nächsten Abschnitt beschrieben.

Feld "Type" in /etc/uucp/Devices-Datei

In diesem Feld wird die Art der Verbindung beschrieben, die das Gerät herstellt. Das UUCP-Feld "Type" kann eines der Schlüsselwörter enthalten, die in den folgenden Abschnitten beschrieben sind.

Schlüsselwort Direct

Das Schlüsselwort Direct steht hauptsächlich in Einträgen für cu -Verbindungen. Dieses Schlüsselwort zeigt an, dass die Verbindung eine direkte Verbindung mit einem anderen Computer oder mit einem Portselektor ist. Erstellen Sie einen separaten Eintrag für jede Zeile, auf die mithilfe der Option -l von cu verwiesen werden soll.

Schlüsselwort ACU

Das Schlüsselwort ACU zeigt an, dass die Verbindung mit einem Remote-Computer (durch cu, UUCP, asppp oder Solaris PPP 4.0) über ein Modem hergestellt wird. Dieses Modem kann entweder direkt mit Ihrem Computer oder indirekt über einen Portselektor verbunden werden.

Portselektor

Der Portselektor ist eine Variable, die im Feld "Type" durch den Namen eines Portselektors ersetzt wird. Portselektoren sind Geräte, die an ein Netzwerk angeschlossen sind, das den Namen eines aufrufenden Modems anfordert und dann Zugriff gewährt. Die Datei /etc/uucp/Dialers enthält Skripten aufrufender Programme für die micom- und develcon-Portselektoren. Sie können Ihre eigenen Portselektoreinträge in die Dialers-Datei einfügen. Weitere Informationen finden Sie unter „ /etc/uucp/Dialers-UUCP-Datei“ auf Seite 612.

System-Name-Variable

Diese Variable wird durch den Namen eines Rechners im Feld "Type" ersetzt, wodurch angezeigt wird, dass die Verbindung eine direkte Verbindung mit dem betreffenden Computer ist. Dieses Naming-Schema wird verwendet, um die Zeile in diesem Devices-Eintrag einem Eintrag in /etc/uucp/Systems für den Computer *System-Name* zuzuordnen.

Typfelder in der Devices-Datei und der Systems-Datei

Beispiel 26–5 zeigt einen Vergleich der Felder in /etc/uucp/Devices und der Felder in /etc/uucp/Systems . Das Schlüsselwort, das im Feld "Type" der Devices -Datei verwendet wird, wird mit dem dritten Feld der Systems-Dateieinträge abgeglichen. In der Devices-Datei weist das Feld "Type" den Eintrag ACUEC auf, der eine automatische Wähleinrichtung angibt, in diesem Fall ein V.32bis-Modem. Dieser Wert wird mit dem Feld "Type" in der

Systems-Datei abgeglichen, in der auch der Eintrag ACUEC enthalten ist. Weitere Informationen finden Sie unter „/etc/uucp/Systems-UUCP-Datei“ auf Seite 597.

BEISPIEL 26–5 Vergleich der Typfelder in der Devices-Datei und der Systems -Datei

Es folgt ein Beispiel für einen Eintrag in der Devices-Datei:

```
ACUEC cua/a - 38400 usrv32bis-ec
```

Es folgt ein Beispiel für einen Eintrag in der Systems-Datei:

```
Arabian Any ACUEC 38400 111222 ogin: Puucp ssword:beledi
```

Feld "Line" in /etc/uucp/Devices-Datei

Dieses Feld enthält den Gerätenamen der Zeile (Port), die dem Devices-Eintrag zugeordnet ist. Wenn das Modem, dass einem bestimmten Eintrag zugeordnet ist, an das /dev/cua/a -Gerät (serieller Port A) angeschlossen wird, muss der in dieses Feld eingegebene Name cua/a lauten. Ein optionales Flag zur Modemsteuerung, M, kann im Feld "Line" verwendet werden, um anzugeben, dass das Gerät verwendet werden kann, ohne auf ein Trägersignal zu warten. Beispiel:

```
cua/a,M
```

Feld "Line2" in /etc/uucp/Devices-Datei

Dieses Feld ist ein Platzhalter. Verwenden Sie hier stets einen Bindestrich (-). Dialer des Typs 801, die nicht im Betriebssystem Solaris unterstützt werden, verwenden das Feld "Line2". Andere Dialer als Typ 801 verwenden diese Konfiguration normalerweise nicht, erfordern aber trotzdem einen Bindestrich in diesem Feld.

Feld "Class" in /etc/uucp/Devices-Datei

Im Feld "Class" wird die Geschwindigkeit des Geräts festgelegt, wenn das Schlüsselwort ACU oder Direct im Feld "Type" verwendet wird. Das Feld "Class" kann jedoch einen Buchstaben und eine Geschwindigkeit (beispielsweise C1200 oder D1200) enthalten, damit zwischen den Klassen von Dialern (z. B. Centrex oder Dimension PBX) unterschieden werden kann.

Diese Unterscheidung ist notwendig, weil viele größere Büros mehrere Arten von Telefonnetzen haben. Ein Netzwerk kann ausschließlich für den internen Gebrauch bestimmt sein, während ein anderes für die externe Kommunikation bestimmt sein kann. In solch einem

Fall müssen Sie unterscheiden, welche Leitung oder welche Leitungen für die interne Kommunikation und welche für die externe Kommunikation verwendet werden sollen.

Das Schlüsselwort, das im Feld "Class" der `Devices` -Datei verwendet wird, wird mit dem Feld "Speed" der `Systems`-Datei abgeglichen.

BEISPIEL 26–6 Feld "Class" in `Devices`-Datei

```
ACU   cua/a   -   D2400  hayes
```

Da manche Geräte mit jeder Geschwindigkeit betrieben werden können, kann im Feld "Class" das Schlüsselwort `Any` angegeben werden. Wenn `Any` angegeben ist, stimmt die Zeile mit jeder Geschwindigkeit überein, die im Feld "Speed" der `Systems`-Datei angefordert wird. Wenn dieses Feld auf `Any` gesetzt ist und das Feld "Speed" der `Systems`-Datei ebenfalls auf `Any` gesetzt ist, beträgt die Geschwindigkeit standardmäßig 2400 Bit/s.

Feld "Dialer-Token-Pairs" in `/etc/uucp/Devices`-Datei

Das Feld "Dialer-Token-Pairs" (DTP) enthält den Namen des Dialers und des Tokens zur Weitergabe des Dialers. Das Feld "DTP" hat folgende Syntax:

dialer token [dialer token]

Der Teil "*dialer*" kann der Name eines Modems oder `direct` oder `uudirect` für ein Direktverbindungsgerät sein. Sie können eine beliebige Anzahl von Dialer-Token-Paaren verwenden. Wenn der Teil "*dialer*" nicht vorhanden ist, wird er einem entsprechenden Eintrag in der `Systems`-Datei entnommen. Der Teil "*token*" kann unmittelbar nach dem Teil "dialer" angegeben werden.

Das letzte Dialer-Token-Paar ist je nach zugehörigem Dialer möglicherweise nicht vorhanden. In den meisten Fällen enthält das letzte Paar nur einen "*dialer*"-Teil. Der Teil "*token*" wird aus dem Feld "Phone" des zugehörigen `Systems`-Dateieintrags abgerufen.

Ein gültiger Eintrag im Teil "*dialer*" kann in der `Dialers`-Datei definiert oder einer von mehreren speziellen Dialertypen sein. Diese speziellen Dialertypen sind in der Software kompiliert und stehen daher zur Verfügung, ohne dass Einträge in der `Dialers`-Datei vorhanden sein müssen. In der folgenden Liste sind spezielle Dialertypen aufgeführt:

`TCP`	TCP/IP-Netzwerk
`TLI`	Transport Level Interface Network (ohne STREAMS)
`TLIS`	Transport Level Interface Network (mit STREAMS)

Weitere Informationen finden Sie unter „Protokolldefinitionen in /etc/uucp/Devices-Datei“ auf Seite 611.

Struktur des Felds "Dialer-Token-Pairs" in /etc/uucp/Devices-Datei

Das Feld "DTP" kann je nach Gerät, das dem Eintrag zugeordnet ist, auf vier verschiedene Arten strukturiert werden.

Es folgt die erste Art der Strukturierung eines solchen Felds:

Direkt verbundenes Modem – Wenn ein Modem direkt mit einem Port Ihres Computer verbunden ist, ist im Feld "DTP" des entsprechenden `Devices`-Dateieintrags nur ein Paar enthalten. Dieses Paar ist normalerweise der Name des Modems. Dieser Name wird verwendet, um den entsprechenden `Devices`-Dateieintrag mit einem Eintrag in der `Dialers` -Datei abzugleichen. Aus diesem Grund muss das Feld "Dialer" mit dem ersten Feld eines `Dialers`-Dateieintrags übereinstimmen.

BEISPIEL 26–7 Feld "Dialers" für ein direkt verbundenes Modem

```
Dialers   hayes =,-,  ""          \\dA\pTE1V1X1Q0S2=255S12=255\r\c
                                  \EATDT\T\r\c CONNECT
```

Beachten Sie, dass nur der Teil "Dialer" (`hayes`) im Feld "DTP" des `Devices`-Dateieintrags vorhanden ist. Das bedeutet, dass das *token*, das an den Dialer (in diesem Fall die Telefonnummer) weitergegeben wird, dem Feld "Phone" eines `Systems` -Dateieintrags entnommen wird. (`\T` wird einbezogen, wie in Beispiel 26–9 beschrieben.)

Es folgen die zweite und dritte Art der Strukturierung des Felds "DTP":

- **Direkte Verbindung** – Für eine direkte Verbindung mit einem bestimmten Computer muss im Feld "DTP" das Schlüsselwort `direct` angegeben sein. Diese Bedingung gilt für beide Arten von Direktverbindungseinträgen, `Direct` und *System-Name* . Lesen Sie dazu „Feld "Type" in /etc/uucp/Devices-Datei“ auf Seite 606.
- **Computer am selben Portselektor** – Wenn ein Computer, mit dem kommuniziert werden soll, sich am selben Portselektor-Switch wie Ihr Computer befindet, muss Ihr Computer zunächst auf den Switch zugreifen. Der Switch stellt dann die Verbindung mit dem anderen Computer her. Dieser Eintragstyp enthält nur ein Paar. Der Teil "*dialer*" wird verwendet, um einen `Dialers`-Dateieintrag abzugleichen.

BEISPIEL 26–8 UUCP-Feld "Dialers" für Computer am selben Portselektor

```
Dialers    develcon ,""   ""           \pr\ps\c est:\007 \E\D\e \007
```

Der Teil "*token* " ist, wie dargestellt, leer. Das bedeutet, dass dieser Teil aus der `Systems`-Datei abgerufen wird. Der `Systems`-Dateieintrag für diesen Computer enthält das Token im Feld "Phone", das normalerweise für die Telefonnummer des Computers reserviert ist. Ausführliche Informationen finden Sie unter „/etc/uucp/Systems-UUCP-Datei“ auf Seite 597. Dieser Typ eines DTP enthält ein Escape-Zeichen (`\D`), das gewährleistet, dass der Inhalt des Felds "Phone" nicht als gültiger Eintrag in der `Dialcodes`-Datei interpretiert wird.

Es folgt die vierte Art der Strukturierung des Felds "DTP":

Modems, die mit einem Portselektor verbunden sind – Wenn ein Hochgeschwindigkeitsmodem mit einem Portselektor verbunden ist, muss Ihr Computer zunächst auf den Portselektor-Switch zugreifen. Der Switch stellt die Verbindung mit dem Modem her. Dieser Eintragstyp erfordert zwei Dialer-Token-Paare. Der Teil "*dialer*" jedes Paars (das fünfte und das siebte Feld des Eintrags) wird verwendet, um die Einträge in der `Dialers`-Datei wie folgt abzugleichen.

BEISPIEL 26–9 UUCP-Feld "dialer" für Modems, die mit einem Portselektor verbunden sind

```
develcon ""     ""    \pr\ps\c  est:\007    \E\D\e      \007
ventel   =&-%   t""   \r\p\r\c  $           <K\T%\r>\c  ONLINE!
```

Im ersten Paar ist `develcon` der Dialer, und `vent` ist das Token, das an den Develcon-Switch weitergegeben wird, um diesem mitzuteilen, welches Gerät (beispielsweise ein Ventel-Modem) mit Ihrem Computer verbunden wird. Dieses Token ist für jeden Portselektor eindeutig, da jeder Switch unterschiedlich konfiguriert werden kann. Nachdem das Ventel-Modem verbunden wurde, wird auf das zweite Paar zugegriffen. Ventel ist der Dialer, und das Token wird aus der `Systems`-Datei abgerufen.

Im Feld "DTP" können zwei Escape-Zeichen enthalten sein:

- `\T` – Zeigt an, dass das Feld "Phone" (*Token*) mithilfe der `/etc/uucp/Dialcodes` -Datei übersetzt werden muss. Dieses Escape-Zeichen wird normalerweise in die `/etc/uucp/Dialers` -Datei für jedes Skript eines aufrufenden Programms eingefügt, das einem Modem (beispielsweise einem Hayes- oder U.S. Robotics-Modem) zugeordnet ist. Darum findet die Übersetzung erst dann statt, wenn auf das Skript des aufrufenden Programms zugegriffen wurde.
- `\D` – Zeigt an, dass das Feld "Phone" (*token*) nicht mithilfe der `/etc/uucp/Dialcodes` -Datei übersetzt werden darf. Wenn kein Escape-Zeichen am Ende eines `Devices` -Eintrags angegeben ist, wird `\D` (Standardeinstellung) verwendet. Das Escape-Zeichen `\D` wird auch in der `/etc/uucp/Dialers` -Datei verwendet, die Einträge enthält, die den Netzwerk-Switches `develcon` und `micom` zugeordnet sind.

Protokolldefinitionen in /etc/uucp/Devices-Datei

Sie können das Protokoll definieren, das in Verbindung mit jedem Gerät in `/etc/uucp/Devices` verwendet werden soll. Diese Angabe ist normalerweise nicht nötig, weil Sie den Standardwert verwenden oder das Protokoll mithilfe des von Ihnen aufgerufenen Systems definieren können. Ausführliche Informationen finden Sie unter „/etc/uucp/Systems-UUCP-Datei“ auf Seite 597. Wenn Sie das Protokoll angeben, muss dies in folgender Form erfolgen:

Type,*Protocol [parameters]*

Sie können beispielsweise `TCP,te` verwenden, um das TCP/IP-Protokoll anzugeben.

In der nachstehenden Tabelle sind die verfügbaren Protokolle für die `Devices` -Datei aufgeführt.

TABELLE 26–2 Protokolle, die in `/etc/uucp/Devices` verwendet werden

Protokoll	Beschreibung
`t`	Dieses Protokoll wird im Allgemeinen für Übertragungen über TCP/IP und andere zuverlässige Verbindungen verwendet. `t` setzt fehlerfreie Übertragungen voraus.
`g`	Dieses Protokoll ist das native Protokoll von UUCP. `g` ist langsam, zuverlässig und zweckmäßig für Übertragungen über stark beanspruchte Telefonleitungen.
`e`	Dieses Protokoll setzt die Übertragung über fehlerfreie Kanäle voraus, die nachrichtenorientiert sind, nicht aber bytestromorientiert wie beispielsweise TCP/IP.
`f`	Dieses Protokoll dient zur Übertragung über X.25-Verbindungen. `f` basiert auf der Flusskontrolle des Datenstroms und dient zur Übertragung über Verbindungen, die (fast) garantiert fehlerfrei sind, insbesondere X.25/PAD-Verbindungen. Eine Prüfsumme wird nur über eine vollständige Datei aktiviert. Wenn eine Übertragung fehlschlägt, kann der Empfänger eine Neuübertragung oder Neuübertragungen anfordern.

Es folgt ein Beispiel für die Zuordnung eines Protokolls zu einem Geräteeintrag:

```
TCP,te - - Any TCP -
```

Dieses Beispiel veranschaulicht, dass Sie versuchen sollten, für `TCP` das `t`-Protokoll zu verwenden. Wenn die Übertragung am anderen Ende der Verbindung abgelehnt wird, verwenden Sie das `e`-Protokoll.

Weder `e` noch `t` sind zur Verwendung über Modems geeignet. Selbst wenn das Modem eine fehlerfreie Übertragung garantiert, kann es dennoch zu einer Unterbrechung der Datenübertragung zwischen dem Modem und der CPU kommen.

/etc/uucp/Dialers-UUCP-Datei

Die /etc/uucp/Dialers-Datei enthält Wählanweisungen für gängige Modems. Sie müssen wahrscheinlich keine Einträge ändern oder dieser Datei hinzufügen, es sei denn, Sie haben vor, ein nicht standardmäßiges Modem zu verwenden oder Ihre UUCP-Umgebung anzupassen. Dennoch sollten Sie nachvollziehen können, was in der Datei enthalten ist und in welcher Beziehung sie zur Systems-Datei und zur Devices-Datei steht.

Der Text gibt den Dialog an, der anfangs über eine Verbindung geführt werden muss, bevor die Verbindung für die Übertragung von Daten zur Verfügung gestellt werden kann. Bei diesem Dialog handelt es sich normalerweise um die Übertragung einer Reihe von erwarteten ASCII-Zeichenfolgen durch das Chat-Skript. Ein Chat-Skript wird oft zum Wählen einer Telefonnummer verwendet.

Wie die unter „ /etc/uucp/Devices-UUCP-Datei“ auf Seite 605 aufgeführten Beispiele zeigen, ist das fünfte Feld in einem Devices-Dateieintrag ein Index, der in die Dialers-Dateien oder auf einen bestimmten Dialertyp wie beispielsweise TCP, TLI oder TLIS verweist. Der uucico-Dämon versucht, das fünfte Feld in der Devices-Datei mit dem ersten Feld jedes Dialers-Dateieintrags abzugleichen. Außerdem wird ab der siebten Position jedes ungeradzahlige Devices-Feld als Index verwendet, der auf die Dialers-Datei verweist. Wenn der Abgleich erfolgreich durchgeführt wird, wird der Dialers -Eintrag interpretiert, wodurch der Dialerdialog durchgeführt werden kann.

Jeder Eintrag in der Dialers -Datei hat folgende Syntax:

```
dialer   substitutions   expect-send
```

Das nachstehende Beispiel zeigt den Eintrag für ein U.S. Robotics-V.32bis-Modem.

BEISPIEL 26–10 Eintrag in /etc/uucp/Dialers -Datei

```
usrv32bis-e    =,-,  ""    dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
                           \EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

usrv32bis-e
: Eintrag im Feld "Dialer". Das Feld "Dialer" dient zum Abgleich des fünften Felds und weiterer ungeradzahliger Felder in der Devices-Datei.

=,-, ""
: Eintrag im Feld "Substitutions". Das Feld "Substitutions" ist eine Übersetzungszeichenfolge. Das erste Zeichen wird dem zweiten Zeichen des Paars zugeordnet. Diese Zuordnung wird normalerweise verwendet, um = und - in eine Zeichenfolge zu übersetzen, die vom Dialer für "Warten auf Wählton" und "Pause" benötigt wird.

dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
: Eintrag im Feld "Expect-Send". Die Expect-Send-Felder sind Zeichenfolgen.

```
\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

Weitere Informationen zum Feld "Expect-Send".

Das folgende Beispiel zeigt Einträge in der `Dialers`-Datei, die definiert werden, wenn Sie UUCP als Teil des Solaris-Installationsprogramms installieren.

BEISPIEL 26–11 Auszüge aus `/etc/uucp/Dialers`

```
penril    =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK

ventel    =&-%    "" \r\p\r\c $ <K\T%%\r>\c ONLINE!

vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE

develcon    ""    "" \pr\ps\c est:\007

\E\D\e \n\007 micom    ""    "" \s\c NAME? \D\r\c GO

hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

#   Telebit TrailBlazer
tb1200    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=2\r\c OK\r
\EATDT\T\r\c CONNECT\s1200
tb2400    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=3\r\c OK\r
\EATDT\T\r\c CONNECT\s2400
tbfast    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=255\r\c OK\r
\EATDT\T\r\c CONNECT\sFAST

# USrobotics, Codes, and DSI modems

dsi-ec  =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts,crtsxoff

dsi-nec =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E0*F3*M1*S1\r\c OK\r \EATDT\T\r\c CONNECT
STTY=crtscts,crtsxoff

usrv32bis-ec =,-,  "" \dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r \EATDT\T\r\c
CONNECT\s14400/ARQ STTY=crtscts,crtsxoff

usrv32-nec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A0&H1&M0&B0&W\r\c OK\r \EATDT\T\r\c
CONNECT STTY=crtscts,crtsxoff

codex-fast =,-, "" \dA\pT&C1&D2*MF0*AA1&R1&S1*DE15*FL3S2=255S7=40S10=40*TT5&W\r\c OK\r
\EATDT\T\r\c CONNECT\s38400 STTY=crtscts,crtsxoff

tb9600-ec =W-,  "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6\r\c OK\r
\EATDT\T\r\cCONNECT\s9600 STTY=crtscts,crtsxoff

tb9600-nec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6S180=0\r\c OK\r \EATDT\T\r\c
CONNECT\s9600 STTY=crtscts,crtsxoff
```

In der folgenden Tabelle werden Escape-Zeichenfolgen aufgelistet, die üblicherweise in den Sendezeichenfolgen in der `Dialers`-Datei verwendet werden.

TABELLE 26–3 Umgekehrter Schrägstrich für `/etc/uucp/Dialers`

Zeichen	Beschreibung
`\b`	Sendet oder erwartet ein Rückschrittzeichen.
`\c`	Kein Zeilenvorschub oder Wagenrücklauf
`\d`	Verzögert um etwa 2 Sekunden.
`\D`	Telefonnummer oder Token ohne `Dialcodes`-Übersetzung
`\e`	Deaktiviert die Echoprüfung.
`\E`	Aktiviert die Echoprüfung für langsame Geräte.
`\K`	Fügt ein Break-Zeichen ein.
`\n`	Sendet einen Zeilenvorschub.
`\nnn`	Sendet Oktalzahlen. Weitere Escape-Zeichen, die verwendet werden können, sind im Abschnitt „`/etc/uucp/Systems`-UUCP-Datei“ auf Seite 597 aufgeführt.
`\N`	Sendet oder erwartet ein NULL-Zeichen (ASCII NUL).
`\p`	Pause von etwa 12 bis 14 Sekunden
`\r`	Rücksprung
`\s`	Sendet oder erwartet ein Leerzeichen.
`\T`	Telefonnummer oder Token mit `Dialcodes`-Übersetzung

Es folgt ein `penril`-Eintrag in der `Dialers`-Datei:

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

Zunächst wird der Ersetzungsmechanismus für das Telefonnummernargument eingerichtet, wodurch = durch `W` (Warten auf Wählton) und - durch `P` (Pause) ersetzt werden.

Der Handshake, der durch den übrigen Teil der Zeile angegeben wird, funktioniert wie folgt:

- `""` – wartet nicht, d. h., der nächste Schritt wird durchgeführt.
- `\d` – verzögert um 2 Sekunden und sendet anschließend ein Wagenrücklaufzeichen.
- `>` – wartet auf ein `>`.
- `Q\c` – sendet ein `Q` ohne Wagenrücklaufzeichen.
- `:` – erwartet ein `:`.
- `\d-` – verzögert um 2 Sekunden und sendet anschließend ein `-` und ein Wagenrücklaufzeichen.
- `>` – wartet auf `>`.

- `s\p9\c` – sendet ein `s`, pausiert und sendet eine `9` ohne Wagenrücklaufzeichen.
- `)-W\p\r\ds\p9\c-)` – wartet auf ein `)`. Wenn `)` nicht empfangen wird, wird die Zeichenfolge wie folgt zwischen den `-`-Zeichen verarbeitet: Sendet ein `W`, pausiert, sendet ein Wagenrücklaufzeichen, verzögert, sendet ein `s`, pausiert, sendet eine `9` ohne Wagenrücklaufzeichen und wartet dann auf das `)`-Zeichen.
- `y\c` – sendet ein `y` ohne Wagenrücklaufzeichen.
- `:` – wartet auf einen Doppelpunkt (`:`).
- `\E\TP` – `\E` aktiviert die Echoprüfung. Wenn von diesem Punkt an ein Zeichen übertragen wird, wartet das UUCP auf den Empfang des Zeichens, bevor es fortfährt. Anschließend sendet das UUCP die Telefonnummer. Das `\T` bedeutet, dass die Telefonnummer verwendet werden soll, die als Argument weitergegeben wird. Durch das `\T` werden die `Dialcodes`-Übersetzung und die Modemfunktionsübersetzung angewandt, die durch das Feld 2 dieses Eintrags angegeben ist. Anschließend sendet `\T` ein `P` und ein Wagenrücklaufzeichen.
- `>` – wartet auf `>`.
- `9\c` – sendet ein `9` ohne ein Zeilenvorschubzeichen.
- `OK` – wartet auf die Zeichenfolge `OK`.

Aktivieren der Hardware-Flusskontrolle in `/etc/uucp/Dialers` -Datei

Sie können auch die `STTY=`*value*-Pseudo-Sendezeichenfolge verwenden, um Modemeigenschaften zu definieren. Die abgehende Hardware-Flusskontrolle kann beispielsweise mit `STTY=crtscts` aktiviert werden. Mit `STTY=crtsxoff` kann die eingehende Hardware-Flusskontrolle aktiviert werden. Mit `STTY=crtscts,crtsxoff` kann sowohl die abgehende als auch die eingehende Hardware-Flusskontrolle aktiviert werden.

`STTY` akzeptiert alle `stty`-Modi. Weitere Informationen finden Sie auf den Manpages `stty(1)` und `termio(7I)`.

Im folgenden Beispiel wird die Hardware-Flusskontrolle in einem `Dialers`-Eintrag aktiviert:

```
dsi =,–, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

Diese Pseudo-Sendezeichenfolge kann auch in Einträgen in der `Systems`-Datei verwendet werden.

Einstellen der Parität in /etc/uucp/Dialers -Datei

In manchen Fällen müssen Sie die Parität zurücksetzen, weil das von Ihnen aufgerufene System die Portparität prüft und die Verbindung unterbricht, wenn die Parität falsch ist. Das expect-send-Paar P_ZERO setzt die Parität auf null:

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r\EATDT\T\r\c CONNECT
```

Es folgen Paritätspaare, die dem expect-send-Paar nachgestellt sein können:

"" P_EVEN Setzt die Parität auf gerade Werte (Standardeinstellung).

"" P_ODD Setzt die Parität auf ungerade Werte.

"" P_ONE Setzt die Parität auf eins.

Diese Pseudo-Sendezeichenfolge kann auch in den Einträgen in der Systems-Datei verwendet werden.

Weitere grundlegende UUCP-Konfigurationsdateien

Sie können die in diesem Abschnitt aufgeführten Dateien zusätzlich zur Systems-, Devices- und Dialers -Datei verwenden, wenn Sie eine grundlegende UUCP-Konfiguration durchführen.

/etc/uucp/Dialcodes-UUCP-Datei

Mithilfe der /etc/uucp/Dialcodes -Datei können Sie Wählcodekürzel definieren, die im Feld "Phone" der /etc/uucp/Systems-Datei verwendet werden können. Sie können die Dialcodes-Datei verwenden, um zusätzliche Informationen zu einer Basistelefonnummer bereitzustellen, die von mehreren Systemen am selben Standort verwendet wird.

Jeder Eintrag hat folgende Syntax:

```
Abbreviation   Dial-Sequence
```

Abkürzung Dieses Feld enthält die Abkürzung, die im Feld "Phone" der Systems-Datei verwendet wird.

Wählsequenz Dieses Feld enthält die Wählsequenz, die an den Dialer weitergegeben wird, wenn auf den betreffenden Systems-Dateieintrag zugegriffen wird.

Vergleichen Sie die Felder in den beiden Dateien. Es folgen die Felder, die in der Dialcodes-Datei enthalten sind:

```
Abbreviation    Dial-Sequence
```

Es folgen die Felder, die in der `Systems`-Datei enthalten sind:

```
System-Name   Time   Type   Speed   Phone   Chat Script
```

Die nachstehende Tabelle enthält Beispielinhalte für die Felder in einer `Dialcodes`-Datei.

TABELLE 26–4 Einträge in der `Dialcodes`-Datei

Kürzel	Wählsequenz
`NY`	`1=212`
`jt`	`9+847`

Der in der ersten Zeile stehende Eintrag NY ist das Kürzel, das im Feld "Phone" der `Systems`-Datei angezeigt wird. Beispielsweise kann die `Systems`-Datei den folgenden Eintrag aufweisen:

```
NY5551212
```

Wenn `uucico` den Eintrag `NY` in der `Systems`-Datei liest, durchsucht `uucico` die `Dialcodes` -Datei nach `NY` und ruft die Wählsequenz `1=212` ab. `1=212` ist die Wählsequenz, die für jeden Anruf nach New York City benötigt wird. Diese Sequenz enthält die Zahl `1`, ein Gleichheitszeichen (`=`), was bedeutet, dass auf einen zweiten Wählton und die Vorwahl `212` gewartet wird. `uucico` sendet diese Informationen an den Dialer und gibt anschließend die `Systems`-Datei für den übrigen Teil der Telefonnummer (`5551212`) zurück.

Der Eintrag `jt 9=847-` funktioniert in Verbindung mit einem Phone-Feldeintrag wie beispielsweise `jt7867` in der `Systems` -Datei. Wenn `uucico` den Eintrag liest, in dem `jt7867` in der `Systems`-Datei angegeben ist, sendet `uucico` die Sequenz `9=847-7867` an den Dialer, wenn das Token im Dialer-Token-Paar `\T` ist.

`/etc/uucp/Sysfiles`-UUCP-Datei

Mithilfe der `/etc/uucp/SysDateis` -Datei können Sie verschiedene Dateien zuweisen, die von `uucp` und `cu` als `Systems-`, `Devices-` und `Dialers` -Dateien verwendet werden. Weitere Informationen zu `cu` finden Sie auf der Manpage cu(1C). Sie können `Sysfiles` für Folgendes verwenden:

- Verschiedene `Systems` -Dateien: Anforderungen von Anmeldeservices können an verschiedene Adressen gesendet werden, anstatt sie an `uucp`-Services zu senden.
- Verschiedene `Dialers` -Dateien: Sie können verschiedene Handshake-Vorgänge für `cu` und `uucp` durchführen.
- Mehrere `Systems` -, `Dialers-` und `Devices`-Dateien: Insbesondere die `Systems`-Datei kann groß werden. Daher ist es sinnvoll, die Datei in mehrere kleine Dateien aufzuteilen.

Die `Sysfiles` -Datei hat folgende Syntax:

```
service=w systems=x:x dialers=y:y devices=z:z
```

w Stellt `uucico` , `cu` oder beide Befehle dar, die durch einen Doppelpunkt getrennt werden.

x Stellt eine oder mehrere Dateien dar, die als `Systems` -Datei verwendet werden. Die Dateinamen werden durch einen Doppelpunkt getrennt und in der angegebenen Reihenfolge gelesen.

y Stellt eine oder mehrere Dateien dar, die als `Dialers` -Datei verwendet werden.

z Stellt eine oder mehrere Dateien dar, die als `Devices` -Datei verwendet werden.

Es wird vorausgesetzt, dass sich jeder Dateiname auf das `/etc/uucp`-Verzeichnis bezieht, wenn kein vollständiger Pfad angegeben ist.

Im folgenden Beispiel, `/etc/uucp/Sysfiles`, wird eine lokale `Systems`-Datei (`Local_Systems`) zusätzlich zur standardmäßigen `/etc/uucp/Systems` -Datei definiert:

```
service=uucico:cu systems=Systems :Local_Systems
```

Wenn dieser Eintrag in `/etc/uucp/Sysfiles` enthalten ist, suchen sowohl `uucico` als auch `cu` zunächst in der standardmäßigen `/etc/uucp/Systems`-Datei. Wenn das aufgerufene System keinen Eintrag in dieser Datei hat oder die Einträge in der Datei nicht funktionieren, prüfen beide Befehle die Datei `/etc/uucp/Local_Systems`.

Wie im vorangegangenen Beispiel zu sehen ist, verwenden `cu` und `uucico` gemeinsam die `Dialers`- und `Devices`-Dateien.

Wenn verschiedene `Systems` -Dateien für die `uucico`- und `cu`-Services definiert sind, werden auf Ihrem Rechner zwei verschiedene Listen von `Systems` gespeichert. Sie können die `uucico` Liste mithilfe des Befehls `uuname` oder die `cu`-Liste mithilfe des Befehls `uuname - C` ausgeben. Es folgt ein weiteres Beispiel für die Datei, das zeigt, dass zuerst die alternativen Dateien und dann je nach Bedarf die Standarddateien abgefragt werden:

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
  service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

`/etc/uucp/Sysname`-UUCP-Datei

Jeder Rechner, der UUCP verwendet, muss einen Namen zur Identifizierung haben. Dieser Name wird oft als *Knotenname* bezeichnet. Der Knotenname erscheint zusammen mit dem Chat-Skript und anderen Zuordnungsinformationen in der `/etc/uucp/Systems` -Datei des

Remote-Rechners. Normalerweise verwendet das UUCP denselben Knotennamen wie den, der durch den `uname -n`-Befehl zurückgegeben wird und auch von TCP/IP verwendet wird.

Sie können einen UUCP-Knotennamen unabhängig vom TCP/IP-Hostnamen angeben, indem Sie die `/etc/uucp/Sysname` -Datei erstellen. Die Datei hat einen einzeiligen Eintrag, in dem der UUCP-Knotenname für Ihr System enthalten ist.

/etc/uucp/Permissions-UUCP-Datei

Die `/etc/uucp/Permissions` -Datei gibt die Berechtigungen an, die von Remote-Computern für die Anmeldung, den Dateizugriff und die Ausführung von Befehlen verwendet werden. Manche Optionen beschränken die Fähigkeit des Remote-Computers, Dateien anzufordern und Dateien zu empfangen, die vom lokalen Rechner in eine Warteschlange gestellt wurden. Es steht eine weitere Option zur Verfügung, die zur Angabe von Befehlen dient, die von einem Remote-Rechner auf dem lokalen Computer ausgeführt werden können.

UUCP-Strukturierungseinträge

Jeder Eintrag ist eine logische Zeile, und physische Zeilen werden von einem umgekehrten Schrägstrich (\) abgeschlossen, wodurch eine Fortsetzung angezeigt wird. Die Einträge bestehen aus Optionen, die durch ein Leerzeichen getrennt werden. Jede Option ist ein Name-Wert-Paar mit folgendem Format:

name=value

Values können durch Doppelpunkt getrennte Listen sein. Innerhalb eines Optionseintrags sind keine Leerzeichen zugelassen.

Kommentarzeilen beginnen mit einem Nummernzeichen (#) und nehmen die gesamte Zeile bis zu einem Zeilenvorschubzeichen ein. Leere Zeilen werden ignoriert, was auch dann der Fall ist, wenn sie innerhalb von mehrzeiligen Einträgen zu finden sind.

Folgende `Permissions`-Dateieinträge werden verwendet:

- `LOGNAME` – gibt die Berechtigungen an, die wirksam werden, wenn ein Remote-Computer sich bei Ihrem Computer anmeldet (bzw. diesen aufruft).

  Hinweis – Wenn Sie einen Aufruf von einem Remote-Rechner erhalten, ist dessen Identität nicht bekannt, es sei denn, der Rechner verfügt über eindeutige Anmeldeinformationen und ein verifizierbares Passwort.

- MACHINE – gibt die Berechtigungen an, die wirksam werden, wenn Ihr Computer sich bei einem Remote-Computer anmeldet (bzw. diesen aufruft).

LOGNAME-Einträge enthalten eine LOGNAME-Option. MACHINE-Einträge enthalten eine MACHINE-Option. Ein Eintrag kann beide Optionen enthalten.

Überlegungen zu UUCP

Wenn Sie die Permissions -Datei verwenden, um den Zugriff zu beschränken, der Remote-Computern gewährt wird, sollten Sie Folgendes berücksichtigen:

- Alle Anmelde-IDs, die von Remote-Computern zum Anmelden für die UUCP-Kommunikation verwendet werden, dürfen nur in einem einzigen LOGNAME-Eintrag enthalten sein.
- Jeder Standort, der mit einem Namen aufgerufen wird, der nicht in einem MACHINE-Eintrag enthalten ist, hat folgende standardmäßige Berechtigungen oder Beschränkungen:
  - Lokale Sende- und Empfangsanforderungen werden ausgeführt.
  - Der Remote-Computer kann Dateien an das /var/spool/uucppublic-Verzeichnis Ihres Computers senden:
  - Die Befehle, die vom Remote-Rechner gesendet und auf Ihrem Computer ausgeführt werden, müssen zu den Standardbefehlen gehören, beispielsweise rmail.

REQUEST-UUCP-Option

Wenn ein Remote-Computer Ihren Computer aufruft und eine Datei anfordert, kann diese Anforderung gewährt oder abgelehnt werden. Die REQUEST-Option gibt an, ob der Remote-Computer Dateiübertragungen von Ihrem Computer anfordern kann. Die Zeichenfolge REQUEST=yes gibt an, dass der Remote-Computer Dateiübertragungen von Ihrem Computer anfordern kann. Die Zeichenfolge REQUEST=no gibt an, dass der Remote-Computer keine Dateiübertragungen von Ihrem Computer anfordern kann. REQUEST=no , die Standardeinstellung, wird verwendet, wenn die REQUEST -Option nicht angegeben ist. Die REQUEST-Option kann entweder in einem LOGNAME-Eintrag angegeben sein, wodurch Ihr Rechner vom Remote-Computer aufgerufen wird, oder in einem MACHINE-Eintrag, wodurch Ihr Rechner den Remote-Computer aufruft.

SENDFILES-UUCP-Option

Wenn ein Remote-Computer Ihren Computer aufruft und dessen Arbeit verrichtet, kann der Remote-Computer versuchen, die Arbeit abzurufen, die Ihr Computer für den

Remote-Computer in die Warteschlange gestellt hat. Mit der SENDFILES-Option wird angegeben, ob Ihr Computer die für den Remote-Computer in die Warteschlange gestellte Arbeit senden kann.

Mit der Zeichenfolge SENDFILES=yes wird angegeben, dass Ihr Computer die für den Remote-Computer in die Warteschlange gestellten Arbeiten senden kann, sofern der Remote-Computer mit einem der Namen angemeldet ist, die in der LOGNAME-Option angegeben sind. Diese Zeichenfolge ist *obligatorisch*, wenn Sie Never in das Feld "Time" von /etc/uucp/Systems eingegeben haben. Dadurch wird Ihr lokaler Rechner in den passiven Modus versetzt. Ihrem Rechner ist jedoch erlaubt, einen Aufruf an den Remote-Computer zu initiieren. Weitere Informationen finden Sie unter „/etc/uucp/Systems-UUCP-Datei“ auf Seite 597.

Die Zeichenfolge SENDFILES=call gibt an, dass Dateien, die auf Ihrem Rechner in die Warteschlange gestellt wurden, nur dann gesendet werden, wenn Ihr Computer den Remote-Computer aufruft. Der call -Wert ist der Standardwert für die SENDFILES-Option. Diese Option ist nur in LOGNAME-Einträgen signifikant, weil MACHINE-Einträge wirksam werden, wenn Aufrufe an Remote-Computer gesendet werden. Wenn die Option in Verbindung mit einem MACHINE -Eintrag verwendet wird, wird sie ignoriert.

MYNAME-UUCP-Option

Anhand dieser Option können Sie einen eindeutigen UUCP-Knotennamen für Ihren Computer festlegen, der neben seinem TCP/IP-Hostnamen Gültigkeit hat, wenn er durch Ausführen des hostname-Befehls zurückgegeben wird. Wenn Sie beispielsweise Ihrem Host versehentlich denselben Namen wie einem anderen System gegeben haben, können Sie die MYNAME-Option der Permissions-Datei definieren. Angenommen, Ihre Organisation soll unter dem Namen widget geführt werden. Wenn alle Ihre Modems mit einem Rechner mit dem Hostnamen gadget verbunden sind, kann ein Eintrag wie der folgende in gadgets Permissions-Datei enthalten sein:

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
  devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
  dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

Jetzt kann sich das System world beim Rechner gadget in gleicher Weise wie bei widget anmelden. Damit der Rechner world Sie auch unter dem Aliasnamen widget kennt, wenn Sie ihn aufrufen, kann für Sie ein Eintrag wie der folgende angegeben sein:

```
MACHINE=world MYNAME=widget
```

Sie können die MYNAME-Option auch für Testzwecke verwenden, da diese Option erlaubt, dass sich Ihr Rechner selbst aufrufen kann. Da diese Option jedoch verwendet werden kann, um die wirkliche Identität eines Rechners zu verbergen, sollten Sie die VALIDATE-Option in der Weise verwenden, die unter „VALIDATE-UUCP-Option“ auf Seite 625 beschrieben ist.

UUCP-READ- und -WRITE-Optionen

Mithilfe dieser Optionen werden verschiedene Teile des Dateisystems angegeben, das von uucico gelesen und beschrieben werden kann. Sie können READ- und WRITE-Optionen entweder mit MACHINE- oder LOGNAME-Einträge benennen.

Das Standardverzeichnis für READ- und WRITE-Optionen ist das uucppublic-Verzeichnis, wie in den folgenden Zeichenfolgen angegeben ist:

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

Die Zeichenfolgen READ=/ und WRITE=/ geben die Berechtigung und den Zugriff für jede Datei an, auf die ein lokaler Benutzer mit Berechtigungen des Typs "Other" (Sonstige) zugreifen kann.

Der Wert dieser Einträge ist eine durch Doppelpunkt getrennte Liste von Pfadnamen. Die READ-Option dient zum Anfordern von Dateien, und die WRITE-Option dient zum Ablegen von Dateien. Einer der Werte muss das Präfix eines vollständigen Pfadnamens einer eingehenden oder abgehenden Datei sein. Um eine Berechtigung zum Ablegen von Dateien in /usr/news sowie im öffentlichen Verzeichnis zu gewähren, verwenden Sie die folgenden Werte in Verbindung mit der WRITE-Option:

```
WRITE=/var/spool/uucppublic:/usr/news
```

Wenn die READ- und WRITE-Optionen verwendet werden, müssen alle Pfadnamen angegeben werden, weil die Pfadnamen nicht in der Standardliste enthalten sind. Wenn beispielsweise der /usr/news-Pfadname der einzige angegebene Pfad in einer WRITE-Option ist, wird keine Berechtigung zum Ablegen von Dateien im öffentlichen Verzeichnis gewährt.

Überlegen Sie gut, welche Verzeichnisse Sie zum Lesen und Beschreiben für Remote-Systeme freigeben. Beispielsweise enthält das /etc-Verzeichnis viele wichtige Systemdateien. Remote-Benutzer sollten nicht berechtigt sein, Dateien in diesem Verzeichnis abzulegen.

UUCP-NOREAD- und NOWRITE-Optionen

Die NOREAD - und NOWRITE -Optionen geben Ausnahmen für die READ- und WRITE-Optionen oder Standardwerte an. Der folgende Eintrag ermöglicht das Lesen und Beschreiben aller

Dateien mit Außnahme der im /etc-Verzeichnis (und den zugehörigen Unterverzeichnissen) gespeicherten Dateien. Beachten Sie, dass diese Optionen Präfixe sind.

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

Dieser Eintrag ermöglicht nur das Beschreiben des standardmäßigen /var/spool/uucppublic -Verzeichnisses. NOWRITE funktioniert auf die gleiche Weise wie die NOREAD-Option. Sie können die NOREAD - und NOWRITE -Optionen sowohl in LOGNAME - als auch in MACHINE-Einträgen verwenden.

CALLBACK-UUCP-Option

Sie können die CALLBACK-Option in LOGNAME-Einträgen verwenden, um anzugeben, dass keine Transaktionen stattfinden, bis das aufrufende System zurückgerufen wird. CALLBACK wird aus folgenden Gründen verwendet:

- Aus Sicherheitsgründen: Wenn Sie einen Rechner zurückrufen, können Sie sicher sein, dass es der richtige Rechner ist.
- Aus Kostengründen: Wenn Sie lange Datenübertragungen ausführen, können Sie einen Rechner auswählen, der für längere Aufrufe vorgesehen ist.

Die Zeichenfolge CALLBACK=yes gibt an, dass Ihre Computer den Remote-Computer zurückrufen muss, bevor Dateiübertragungen stattfinden.

Die Standardeinstellung der CALLBACK-Option ist CALLBACK=no. Wenn Sie CALLBACK auf yes setzen, müssen die Berechtigungen, die sich auf den übrigen Dialog beziehen, im MACHINE -Eintrag angegeben sein, der dem aufrufenden System entspricht. Geben Sie diese Berechtigungen nicht im LOGNAME- oder LOGNAME-Eintrag an, den der Remote-Rechner für Ihren Host definiert haben kann.

Hinweis – Wenn zwei Standorte füreinander die CALLBACK-Option angegeben haben, wird der Dialog nie eingeleitet.

COMMANDS-UUCP-Option

Achtung – Die COMMANDS -Option kann die Sicherheit Ihres Systems beeinträchtigen. Verwenden Sie diese Option nur nach sorgfältiger Überlegung.

Sie können die COMMANDS-Option in MACHINE-Einträgen verwenden, um die Befehle anzugeben, die ein Remote-Computer auf Ihrem Computer ausführen kann. Das uux-Programm generiert

Remote-Ausführungsanforderungen und stellt die Anforderungen, die an den Remote-Computer gesendet werden sollen, in eine Warteschlange. Die Übertragung von Dateien und Befehlen an den Zielcomputern für die Remote-Ausführung ist eine Ausnahme zu der Regel, dass `MACHINE` -Einträge nur dann wirksam werden, wenn Ihr System Aufrufe sendet.

Beachten Sie, dass `COMMANDS` nicht in einem `LOGNAME` -Eintrag verwendet wird. `COMMANDS` in `MACHINE`-Einträgen dienen zum Definieren der Befehlsberechtigungen, ob Sie das Remote-System aufrufen oder umgekehrt.

Die Zeichenfolge `COMMANDS=rmail` gibt die Standardbefehle an, die ein Remote-Computer auf Ihrem Computer ausführen kann. Wenn eine Befehlszeichenfolge in einem `MACHINE`-Eintrag verwendet wird, werden die Standardbefehle außer Kraft gesetzt. Beispielsweise wird durch den folgenden Eintrag der COMMAND-Standardbefehl außer Kraft gesetzt, wodurch die Computer `owl`, `raven`, `hawk` und `dove` jetzt `rmail`, `rnews` und `lp` auf Ihrem Computer ausführen können.

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

Zusätzlich zu den gerade angegebenen Namen können Sie vollständige Pfadnamen von Befehlen verwenden. Durch den folgenden Eintrag wird beispielsweise angegeben, dass der Befehl `rmail` den standardmäßigen Suchpfad verwendet.

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

Die standardmäßigen Suchpfade für UUCP sind `/bin` und `/usr/bin`. Wenn der Remote-Computer `rnews` oder `/usr/local/rnews` für den auszuführenden Befehl angibt, wird `/usr/local/rnews` ungeachtet des standardmäßigen Pfads ausgeführt. Dementsprechend ist `/usr/local/lp` der ausgeführte `lp`-Befehl.

Wenn der Wert `ALL` in die Liste einbezogen wird, bedeutet das, dass jeder im Eintrag angegebene Befehl vom Remote-Computer ausgeführt wird. Wenn Sie diesen Wert verwenden, gewähren Sie den Remote-Computern uneingeschränkten Zugriff auf Ihren Rechner.

Achtung – Dieser Wert gewährt weit mehr Zugriffberechtigungen als normale Benutzer haben. Sie sollten diesen Wert nur dann verwenden, wenn sich beide Rechner am selben Standort befinden, in kurzer Entfernung miteinander verbunden sind und die Benutzer vertrauenswürdig sind.

In der folgenden Zeichenfolge wurde der Wert `ALL` hinzugefügt:

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

Diese Zeichenfolge zeigt Folgendes:

- Der Wert `ALL` kann überall in der Zeichenfolge platziert werden.
- Die für `rnews` und `lp` angegebenen Pfadnamen werden (anstelle des standardmäßigen Pfads) verwendet, wenn der angeforderte Befehl nicht die vollständigen Pfadnamen für `rnews` oder `lp` enthält.

Sie sollten die `VALIDATE`-Option verwenden, wenn Sie potentiell gefährliche Befehle verwenden, wie beispielsweise `cat` und `uucp` in Verbindung mit der `COMMANDS`-Option. Jeder Befehl, der Dateien lesen oder beschreiben kann, ist eine potentielle Gefahr für die lokale Sicherheit, wenn der Befehl vom UUCP-Remote-Ausführungsdämon (`uuxqt`) ausgeführt wird.

`VALIDATE`-UUCP-Option

Verwenden Sie die `VALIDATE`-Option in Verbindung mit der `COMMANDS`-Option, wenn Sie Befehle angeben, die möglicherweise die Sicherheit Ihres Rechners gefährden. Die `VALIDATE`-Option ist lediglich eine zusätzliche Sicherheitsstufe zur `COMMANDS`-Option, bietet aber mehr Sicherheit für den Zugriff auf Befehle als `ALL`.

`VALIDATE` bietet einen bestimmten Grad der Verifizierung der Identität des aufrufenden Programms, da der Hostname des aufrufenden Rechners mit dem Anmeldenamen des aufrufenden Rechners abgeglichen wird. Durch die folgende Zeichenfolge wird sichergestellt, dass die Verbindung abgelehnt wird, wenn ein anderer Rechner als `widget` oder `gadget` versucht, sich als `Uwidget` anzumelden.

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

Die `VALIDATE`-Option verlangt von privilegierten Computern eine eindeutige Anmeldung und ein eindeutiges Passwort für UUCP-Transaktionen. Ein wichtiger Aspekt dieser Validierung ist, dass die diesem Eintrag zugeordnete Anmeldung sowie das Passwort geschützt sind. Wenn ein Außenstehender dieser Informationen habhaft wird, kann die Option `VALIDATE` nicht mehr als sicher betrachtet werden.

Erwägen Sie sorgfältig, welchen Remote-Computern Sie privilegierte Anmeldungen und Passwörter für UUCP-Verbindungen gewähren. Wenn Sie einem Remote-Computer ein spezielle Anmeldung und ein Passwort mit Dateizugriff und Remote-Ausführung gewähren, dann wäre das so, als objeder Benutzer des Computers eine normale Anmeldung und ein Passwort für den Zugriff auf Ihren Computer erhält. Wenn Sie also einen Benutzer des Remote-Computers als nicht vertrauenswürdig erachten, gewähren Sie dem Computer weder eine privilegierte Anmeldung noch ein Passwort.

Der folgende `LOGNAME`-Eintrag gibt an, dass ein Remote-Computer, der behauptet, `eagle` , `owl` oder `hawk` zu sein, sich bei Ihrem Computer mit `uucpfriend` anmelden muss:

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

Wenn ein Außenstehender der uucpfriend-Anmeldung und des Passworts habhaft wird, ist eine Täuschung einfach zu bewerkstelligen.

Was aber hat dieser Eintrag mit der COMMANDS-Option zu tun, die nur in MACHINE-Einträgen vorkommt? Dieser Eintrag verknüpft den MACHINE-Eintrag (und die COMMANDS-Option) mit einem LOGNAME-Eintrag, der einer privilegierten Anmeldung zugeordnet ist. Diese Verknüpfung ist erforderlich, weil der Ausführungsdämon nicht aktiv ist, während der Remote-Computer angemeldet ist. Tatsächlich ist die Verknüpfung ein asynchroner Prozess, dem nicht bekannt ist, von welchem Computer die Ausführunganforderung kommt. Darum lautet die Frage: Woher weiß Ihr Computer, woher die Ausführungsdateien kommen?

Jeder Remote-Computer hat ein eigenes Spool-Verzeichnis auf Ihrem lokalen Rechner. Diese Spool-Verzeichnisse haben Schreibberechtigungen, die nur UUCP-Programmen gewährt werden. Die vom Remote-Computer kommenden Ausführungsdateien werden im Spool-Verzeichnis des Remote-Computers abgelegt, nachdem sie auf Ihren Computer übertragen wurden. Wenn der uuxqt-Dämon ausgeführt wird, kann er den Namen des Spool-Verzeichnisses verwenden, um den MACHINE-Eintrag in der Permissions-Datei zu finden und die COMMANDS-Liste abzurufen. Wenn der Name des Computers nicht in der Permissions-Datei enthalten ist, wird die Standardliste verwendet.

Das folgende Beispiel zeigt die Beziehung zwischen den MACHINE- und LOGNAME-Einträgen:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
COMMANDS=rmail:/usr/local/rnews \
READ=/ WRITE=/
LOGNAME=uucpz VALIDATE=eagle:owl:hawk \
REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

Der Wert in der COMMANDS-Option bedeutet, dass Remote-Benutzer rmail und /usr/local/rnews ausführen können.

Im ersten Eintrag müssen Sie davon ausgehen, dass Sie, wenn Sie einen der gelisteten Computer aufrufen wollen, in Wirklichkeit eagle, owl oder hawk aufrufen. Aus diesem Grund werden alle Dateien, die in einem der eagle-, owl - oder hawk-Spool-Verzeichnisse abgelegt werden, von einem dieser Rechner abgelegt. Wenn ein Remote-Rechner sich anmeldet und behauptet, einer dieser drei Rechner zu sein, werden seine Ausführungsdateien ebenfalls im privilegierten Spool-Verzeichnis abgelegt. Darum müssen Sie prüfen, ob der Rechner über die privilegierte Anmeldung uucpz verfügt.

UUCP- MACHINE-Eintrag für OTHER

Sie können verschiedene Optionswerte für Remote-Rechner angeben, die nicht in bestimmten MACHINE-Einträgen enthalten sein. Dies kann nötig sein, wenn viele Rechner Ihren Host

aufrufen und sich der Befehlsdatensatz von Zeit zu Zeit ändert. Der Name OTHER für den Rechnernamen wird für diesen Eintrag verwendet, was im folgenden Beispiel gezeigt wird:

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

Alle anderen Optionen, die für den MACHINE-Eintrag zur Verfügung stehen, können auch für die Rechner definiert werden, die nicht in anderen MACHINE-Einträgen angegeben sind.

Kombinieren der MACHINE- und LOGNAME-Einträge für UUCP

Sie können MACHINE - und LOGNAME-Einträge in einem einzelnen Eintrag kombinieren, sofern die allgemeinen Optionen dieselben sind. Beispielsweise verwenden die beiden folgenden Einträge dieselben REQUEST -, READ- und WRITE-Optionen:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

und

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

Sie können diese Einträge wie folgt zusammenführen:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES-yes \
READ=/ WRITE=/
```

Durch das Kombinieren von MACHINE- und LOGNAME-Einträgen sind die Permissions-Dateien leichter zu handhaben und können effizienter eingesetzt werden.

UUCP-Weiterleitung

Wenn Dateien über eine Reihe von Rechnern übertragen werden, müssen die dazwischen liegenden Rechner über den Befehl uucp in ihren COMMANDS-Optionen verfügen. Wenn Sie den folgenden Befehl eingeben, funktioniert die Weiterleitung nur dann, wenn der Rechner willow dem Rechner oak gestattet, das uucp-Programm auszuführen.

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

Der Rechner oak muss auch Ihrem Rechner gestatten, das uucp-Programm auszuführen. Der Rechner pine, der letzte der benannten Rechner, verfügt nicht über die Berechtigung zur

Ausführung des uucp-Befehls, weil der Rechner keine Weiterleitungen ausführt. Normalerweise sind Rechner nicht auf diese Weise konfiguriert.

UUCP- /etc/uucp/Poll-Datei

Die /etc/uucp/Poll-Datei enthält Informationen für das Aufrufen von Remote-Rechnern. Jeder Eintrag in der Poll -Datei enthält den Namen eines aufzurufenden Remote-Rechners, ein Tabulatorzeichen oder ein Leerzeichen sowie die Stunden, zu denen der Rechner aufgerufen werden soll. Es folgt das Format der Einträge in der Poll-Datei:

sys-name hour ...

Beispielsweise bewirkt der Eintrag **eagle 0 4 8 12 16 20**, dass der Computer eagle alle vier Stunden aufgerufen wird.

Das uudemon.poll-Skript verarbeitet die Poll-Datei, führt aber nicht den Aufruf aus. Das Skript richtet lediglich im Spool-Verzeichnis eine Aufrufarbeitsdatei ein (die immer den Namen C.*file* hat). Das uudemon.poll -Skript startet den Scheduler, und dieser untersucht alle Arbeitsdateien im Spool-Verzeichnis.

UUCP- /etc/uucp/Config-Datei

Mit der /etc/uucp/Config -Datei können Sie bestimmte Parameter manuell außer Kraft setzen. Jeder Eintrag in der Config-Datei hat folgendes Format:

parameter=wert

Eine vollständige Liste der konfigurierbaren Parameternamen finden Sie in der zusammen mit Ihrem System bereitgestellten Config-Datei.

Der folgende Config-Eintrag setzt die standardmäßige Protokollordnungsrelation auf Gge und ändert die G-Protokollstandards in 7 Fenster und 512-Byte-Pakete.

```
Protocol=G(7,512)ge
```

UUCP- /etc/uucp/Grades-Datei

Die /etc/uucp/Grades -Datei enthält die Definitionen für die Jobklassen, die verwendet werden können, um Jobs für einen Remote-Rechner in eine Warteschlange zu stellen. Diese

Datei enthält auch die Berechtigungen für jede Jobklasse. Jeder Eintrag in dieser Datei ist eine Definition eine vom Administrator definierten Jobklasse, die Benutzern erlaubt, Jobs in eine Warteschlange zu stellen.

Jeder Eintrag in der `Grades`-Datei hat folgendes Format:

Benutzerjobklasse Systemjobklasse Jobgröße Berechtigungstyp ID-Liste

Jeder Eintrag enthält Felder, die durch ein Leerzeichen getrennt sind. Das letzte Feld des Eintrags setzt sich aus Unterfeldern zusammen, die ebenfalls durch Leerzeichen getrennt sind. Wenn ein Eintrag mehr als eine physische Zeile einnimmt, können Sie einen umgekehrten Schrägstrich verwenden, um den Eintrag auf der folgenden Zeile fortzusetzen. Kommentarzeilen beginnen mit einem Nummernzeichen (#) und nehmen die gesamte Zeile ein. Leere Zeilen werden immer ignoriert.

UUCP-Feld "User-job-grade"

Dieses Feld enthält einen vom Administrator definierten Benutzerjobklassen-Namen, der aus bis zu 64 Zeichen besteht.

UUCP-Feld "System-job-grade"

Dieses Feld enthält eine aus einem Zeichen bestehende Jobklasse, zu der die *User-job-grade* zugeordnet wird. Die gültigen Zeichen sind A–Z, a–z, wobei A die höchste und z die niedrigste Priorität hat.

Beziehung zwischen Benutzer- und Systemjobklassen

Die Benutzerjobklasse kann mehreren Systemjobklassen zugeordnet sein. Beachten Sie, dass die `Grades`-Datei sequentiell nach Vorkommen einer Benutzerjobklasse durchsucht wird. Darum sollten mehrere Vorkommen einer Systemjobklasse in Übereinstimmung mit der Beschränkung der maximalen Jobgröße aufgelistet werden.

Wenn keine maximale Anzahl für die Benutzerjobklassen angegeben ist, sind maximal 52 Systemjobklassen zugelassen. Der Grund dafür ist, dass mehrere *User-job-grade* einer *System-job-grade* zugeordnet werden können, aber jede *User-job-grade* in der Datei auf einer separaten Zeile stehen muss. Beispiel:

```
mail N Any User Any netnews N Any User Any
```

Wenn diese Konfiguration in einer `Grades`-Datei definiert ist, verwenden diese beiden *User-job-grade*-Felder dieselbe *System-job-grade*. Da die Berechtigung für eine *Job-grade* einer

User-job-grade und nicht einer *System-job-grade* zugeordnet ist, können zwei *User-job-grade* dieselbe *System-job-grade* verwenden und haben zwei verschiedene Berechtigungsdatensätze.

Standardklasse

Sie können die Verknüpfung einer standardmäßigen *User-job-grade* mit einer Systemjobklasse definieren. Sie müssen den Schlüsselwortstandard als Benutzerjobklasse im Feld *User-job-grade* der `Grades` -Datei und die mit ihr verknüpfte Systemjobklasse verwenden. Die Beschränkungen und ID-Felder sollten mit `Any` definiert werden, sodass jeder Benutzer und jeder Job entsprechend dieser Klasse in eine Warteschlange gestellt werden kann. Beispiel:

```
default a Any User Any
```

Wenn Sie keine standardmäßige Benutzerjobklasse definieren, wird die integrierte Standardklasse `Z` verwendet. Da der Standardwert des Beschränkungsfelds `Any` ist, werden mehrere Vorkommen der Standardklasse nicht überprüft.

UUCP-Feld "Job-size"

Dieses Feld gibt die maximale Jobgröße an, die für die Warteschlange eingegeben werden kann. Die *Job-size* wird in Byte gemessen und kann eine Liste der Optionen sein, die in der folgenden Liste aufgeführt sind:

nnnn	Ganzzahl zur Angabe der maximalen Jobgröße für diese Jobklasse
n `K`	Dezimalzahl zur Angabe der Anzahl von Kilobytes (`K` ist eine Abkürzung für Kilobyte)
n `M`	Dezimalzahl zur Angabe der Anzahl von Megabytes (`M` ist eine Abkürzung für Megabyte)
`Any`	Schlüsselwort, das angibt, dass keine maximale Jobgröße vorhanden ist

Es folgen einige Beispiele:

- `5000` stellt 5000 Byte dar
- `10K` stellt 10 KB dar
- `2M` stellt 2 MB dar

UUCP-Feld "Permit-type"

Dieses Feld enthält ein Schlüsselwort, das angibt, wie die ID-Liste interpretiert werden soll. In der nachstehenden Tabelle werden die Schlüsselwörter und ihre Bedeutungen aufgeführt.

TABELLE 26–5 Feld "Permit-type"

Schlüsselwort	Inhalt der ID-Liste
`User`	Anmeldenamen von Benutzern, denen erlaubt ist, diese Jobklasse zu verwenden
`Non-user`	Anmeldenamen von Benutzern, denen nicht erlaubt ist, diese Jobklasse zu verwenden
`Group`	Namen von Gruppen, deren Mitgliedern erlaubt ist, diese Gruppe zu verwenden
`Non-group`	Namen von Gruppen, deren Mitgliedern nicht erlaubt ist, diese Jobklasse zu verwenden

UUCP-Feld "ID-Liste"

Dieses Feld enthält eine Liste mit Anmeldenamen oder Gruppennamen, deren Benutzern gestattet oder verweigert werden soll, für diese Jobklasse Vorgänge in die Warteschlange zu stellen. Die Liste der Namen wird durch ein Leerzeichen getrennt und von einem Zeilenvorschubzeichen abgeschlossen. Das Schlüsselwort `Any` wird verwendet, um anzugeben, dass jedem Benutzer gestattet wird, für diese Jobklasse Vorgänge in die Warteschlange zu stellen.

Weitere UUCP-Konfigurationsdateien

In diesem Abschnitt werden drei weniger häufig modifizierte Dateien beschrieben, die die Verwendung von UUCP-Funktionen beeinflussen.

`/etc/uucp/Devconfig`-UUCP-Datei

Mithilfe der `/etc/uucp/Devconfig` -Datei können Sie Geräte nach Service wie beispielsweise `uucp` oder `cu` konfigurieren. `Devconfig`-Einträge definieren die STREAMS-Module, die für ein bestimmtes Gerät verwendet werden. Diese Einträge haben folgendes Format:

`service=`*x* `device=`*y* `push=`*z*[:*z*...]

x kann `cu`, `uucico` oder beide Services darstellen, die durch einen Doppelpunkt getrennt sind. *y* ist der Name eines Netzwerks, der mit einem Eintrag in der `Devices`-Datei übereinstimmen muss. *z* wird durch die Namen der STREAMS-Module ersetzt, und zwar in der Reihenfolge, in der sie in den Stream eingespeichert werden. Für die `cu`- und `uucp`-Services können verschiedene Module und Geräte definiert werden.

Die folgenden Einträge sind für ein STARLAN-Netzwerk bestimmt und werden am häufigsten in der Datei verwendet:

```
service=cu       device=STARLAN     push=ntty:tirdwr
service=uucico   device=STARLAN     push=ntty:tirdwr
```

In diesem Beispiel wird zunächst `ntty` und dann `tirdwr` eingespeichert.

UUCP- `/etc/uucp/Limits`-Datei

Die `/etc/uucp/Limits` -Datei steuert die maximale Anzahl von gleichzeitigen `uucicos`, `uuxqts` und `uuscheds`, die im `uucp`-Netzwerk ausgeführt werden. In den meisten Fällen können die Standardwerte verwendet werden, und es sind keine Änderungen erforderlich. Wenn Sie die Werte dennoch ändern möchten, verwenden Sie einen Texteditor.

Es folgt das Format der `Limits` -Datei:

`service=`*x* `max=`*y*:

x kann `uucico`, `uuxqt` oder `uusched` sein, und *y* ist das Limit, dass für den Service zugelassen ist. Die Felder können in beliebiger Reihenfolge angeordnet und Kleinbuchstaben sein.

Die folgenden Einträge werden im Allgemeinen in der `Limits` -Datei verwendet:

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

In dem Beispiel werden fünf `uucicos`, fünf `uuxqts` und zwei `uuscheds` auf Ihrem Rechner zugelassen.

UUCP- `remote.unknown`-Datei

Eine weitere Datei, die die Verwendung der Kommunikationsfunktionen beeinflusst, ist die `remote.unknown`-Datei. Diese Datei ist ein Binärprogramm, das ausgeführt wird, falls ein Rechner nicht gefunden wird, wenn eine der `Systems`-Dateien einen Dialog beginnt. Dieses Programm protokolliert den Kommunikationsversuch und unterbricht die Verbindung.

Achtung – Wenn Sie die Berechtigungen der `remote.unknown`-Datei ändern, sodass die Datei nicht ausgeführt werden kann, akzeptiert Ihr System Verbindungen von allen anderen Systemen.

Dieses Programm wird ausgeführt, wenn ein Rechner, der nicht in einer der `Systems`-Datei enthalten ist, einen Dialog beginnt. Das Programm protokolliert den Kommunikationsversuch, kann aber keine Verbindung herstellen. Wenn Sie die Berechtigungen dieser Datei ändern, sodass die Datei nicht ausgeführt werden kann (`chmod 000 remote.unknown`), akzeptiert Ihr System alle Kommunikationsanfragen. Diese Änderung ist nicht trivial. Sie sollten gute Gründe für diese Änderung haben.

UUCP-Verwaltungsdateien

Als Nächstes werden die UUCP-Verwaltungsdateien beschrieben. Diese Dateien werden in Spool-Verzeichnissen erstellt, um Geräte zu sperren, temporäre Daten zu speichern oder Informationen über Remote-Übertragungen oder Remote-Ausführungen aufzubewahren.

- *Temporäre Datendateien* (`TM`) – Diese Datendateien werden durch UUCP-Prozesse unter dem Spool-Verzeichnis `/var/spool/uucp/`*x* erstellt, wenn eine Datei von einem anderen Rechner empfangen wird. Das Verzeichnis *x* hat denselben Namen wie der Remote-Rechner, der die Datei sendet. Die Namen der temporären Datendateien haben folgendes Format:

  `TM.` *pid.ddd*

  pid ist eine Prozess-ID, und *ddd* ist eine sequentielle dreistellige Zahl, die mit 0 beginnt.

  Bei Empfang der gesamten Datei wird die `TM.` *pid.ddd*-Datei auf den Pfad verschoben, dessen Name in der (nachstehend erläuterten) `C.`*sysnxxxx*-Datei angegeben ist, die die Übertragung verursacht hat. Wenn die Verarbeitung vorzeitig abgebrochen wird, kann die `TM.`*pid.ddd* -Datei im *x*-Verzeichnis verbleiben. Diese Dateien werden automatisch durch `uucleanup` entfernt.
- *Sperrdateien* (`LCK`) – Sperrdateien werden für jedes verwendete Geräte im `/var/spool/locks` -Verzeichnis erstellt. Sperrdateien verhindern duplizierte Dialoge und mehrere Versuche, dasselbe aufrufende Gerät zu verwenden. In der nachstehenden Tabelle sind die verschiedenen Typen von UUCP-Sperrdateien aufgeführt.

TABELLE 26–6 UUCP-Sperrdateien

Dateiname	Beschreibung
`LCK.` *sys*	*sys* stellt den Namen des Rechners dar, der die Datei verwendet.
`LCK.` *dev*	*dev* stellt den Namen eines Geräts dar, das die Datei verwendet.
`LCK.`*LOG*	*LOG* stellt eine gesperrte UUCP-Protokolldatei dar.

Diese Dateien können im Spool-Verzeichnis verbleiben, wenn die Kommunikationsverbindung unerwartet abgebrochen wird, beispielsweise bei einem Rechnerabsturz. Die Sperrdatei wird ignoriert (entfernt), nachdem der übergeordnete Prozess nicht mehr aktiv ist. Die Sperrdatei enthält die Prozess-ID des Prozesses, durch den die Sperre erstellt wurde.

- *Arbeitsdatei* (`C.`) – Arbeitsdateien werden in einem Spool-Verzeichnis erstellt, wenn Arbeiten, wie beispielsweise Dateiübertragungen oder Remote-Befehlsausführungen, für einen Remote-Rechner in eine Warteschlange gestellt wurden. Die Namen der Arbeitsdateien haben folgendes Format:

  `C.` *sysnxxxx*

sys ist der Name des Remote-Rechners, *n* ist das ASCII-Zeichen, das die Klasse (Priorität) der Arbeit darstellt, und *xxxx* ist die vierstellige Jobsequenznummer, die durch UUCP zugewiesen wird. Arbeitsdateien enthalten folgende Informationen:

- vollständiger Pfadname der Datei, die gesendet oder angefordert werden soll
- vollständiger Pfadname des Ziels oder Benutzers oder Dateinamens
- Anmeldename des Benutzers
- Liste der Optionen
- Name der zugehörigen Datendateien im Stammverzeichnis. Wenn die `uucp -C` oder `uuto -p`-Option angegeben wurde, wird der Dummy-Name (`D.0`) verwendet.
- Modusbits der Quelldatei.
- Der Anmeldename eines Remote-Benutzers, der nach Abschluss der Übertragung benachrichtigt werden muss.

- *Datendatei*(`D.`) – Datendateien werden erstellt, wenn Sie durch eine Eingabe auf der Befehlszeile die Quelldatei in das Spool-Verzeichnis kopieren. Die Namen der Datendateien haben folgendes Format:

  `D.` *systmxxxxyyy* – *systm* sind die erste fünf Zeichen im Namen des Remote-Rechners. *xxxx* ist eine vierstellige Jobsequenznummer, die durch `uucp` zugewiesen wird. Nach der vierstelligen Jobsequenznummer kann eine nachfolgende Nummer folgen. *yyy* wird verwendet, wenn mehrere `D.`-Dateien für eine Arbeitsdatei (`C.`) erstellt werden.

- `X.` *(Ausführungsdatei)* – Ausführungsdateien werden im Spool-Verzeichnis vor der Ausführung von Remote-Befehlen erstellt. Die Namen der Ausführungsdateien haben folgendes Format:

  `X.` *sysnxxxx*

  sys ist der Name des Remote-Rechners. *n* ist das Zeichen, das die Klasse (Priorität) der Arbeit darstellt. *xxxx* ist eine vierstellige Sequenznummer, die durch UUCP zugewiesen wird. Ausführungsdateien enthalten folgende Informationen:

  - Anmeldung des Anforderers und Rechnername
  - Namen der Dateien, die für die Ausführung benötigt werden
  - Eingabe, die als Standardeingabe für die Befehlszeichenfolge verwendet werden soll
  - Rechner- und Dateiname zum Empfangen der Standardausgabe der Befehlausführung
  - Befehlszeichenfolge
  - Optionszeilen für Rückgabestatusanforderungen

UUCP-Fehlermeldungen

In diesem Abschnitt werden die Fehlermeldungen aufgeführt, die sich auf UUCP beziehen.

UUCP-ASSERT-Fehlermeldungen

In der nachstehenden Tabelle sind ASSERT-Fehlermeldungen aufgeführt.

TABELLE 26–7 ASSERT-Fehlermeldungen

Fehlermeldung	Beschreibung oder Aktion
`CAN'T OPEN`	Ein `open()`- oder `fopen()`-Befehl ist fehlgeschlagenen.
`CAN'T WRITE`	Ein `write()`-, `fwrite()`-, `fprint()`- oder ein ähnlicher Befehl ist fehlgeschlagenen.
`CAN'T READ`	Ein `read()`-, `fgets()`- oder ein ähnlicher Befehl ist fehlgeschlagenen.
`CAN'T CREATE`	Ein `creat()`-Aufruf ist fehlgeschlagenen.
`CAN'T ALLOCATE`	Eine dynamische Zuordnung ist fehlgeschlagenen.
`CAN'T LOCK`	Ein Versuch, eine Sperrung (`LCK`) durchzuführen, ist fehlgeschlagenen. In manchen Fällen kann dies ein schwerwiegender Fehler sein.
`CAN'T STAT`	Ein `stat()`-Aufruf ist fehlgeschlagenen.
`CAN'T CHMOD`	Ein `chmod()`-Aufruf ist fehlgeschlagenen.
`CAN'T LINK`	Ein `link()`-Aufruf ist fehlgeschlagenen.
`CAN'T CHDIR`	Ein `chdir()`-Aufruf ist fehlgeschlagenen.
`CAN'T UNLINK`	Ein `unlink()`-Aufruf ist fehlgeschlagenen.
`WRONG ROLE`	Dies ist ein internes Logikproblem.
`CAN'T MOVE TO CORRUPTDIR`	Ein Versuch, fehlerhafte `C.`- oder `X.`-Dateien in das `/var/spool/uucp/.Corrupt`-Verzeichnis zu verschieben, ist fehlgeschlagenen. Das Verzeichnis ist wahrscheinlich nicht vorhanden oder hat falsche Modi oder einen falschen Eigentümer.
`CAN'T CLOSE`	Ein `close()`- oder `fclose()`-Aufruf ist fehlgeschlagenen.
`FILE EXISTS`	Es wurde versucht, eine `C.`- oder `D.`-Datei zu erstellen, aber die Datei ist bereits vorhanden. Dieser Fehler tritt auf, wenn ein Problem mit dem sequentiellen Dateizugriff entsteht, was für gewöhnlich auf einen Softwarefehler hindeutet.
`NO uucp SERVICE NUMBER`	Es wird versucht, einen TCP/IP-Aufruf durchzuführen, aber es ist kein Eintrag in `/etc/services` für UUCP vorhanden.
`BAD UID`	Die Benutzer-ID ist nicht in der Passwortdatenbank enthalten. Prüfen Sie die Name Service-Konfiguration.

TABELLE 26–7 ASSERT-Fehlermeldungen *(Fortsetzung)*

Fehlermeldung	Beschreibung oder Aktion
`BAD LOGIN_UID`	Siehe obige Beschreibung.
`BAD LINE`	In der `Devices` -Datei ist eine ungültige Zeile enthalten. Nicht genügend Argumente auf einer oder mehreren Zeilen
`SYSLST OVERFLOW`	Eine interne Tabelle in `gename.c` ist übergelaufen. Ein einzelner Job hat versucht, mit mehr als 30 Systemen zu kommunizieren.
`TOO MANY SAVED C FILES`	Siehe obige Beschreibung.
`RETURN FROM fixline ioctl`	Ein `ioctl(2)`-Vorgang, der nie fehlschlagen sollte, ist fehlgeschlagenen. Ein Systemtreiberproblem ist aufgetreten.
`BAD SPEED`	Eine ungültige Geschwindigkeit ist in der `Devices`- oder `Systems`-Datei (Feld "Class" oder "Speed") angegeben.
`BAD OPTION`	In der `Permissions`-Datei ist eine ungültige Zeile oder Option enthalten. Dieser Fehler muss sofort beseitigt werden.
`PKCGET READ`	Der Remote-Rechner hängt wahrscheinlich. Es ist keine Aktion erforderlich.
`PKXSTART`	Der Remote-Rechner hat den Vorgang abgebrochen und der frühere Zustand kann nicht wiederhergestellt werden. Dieser Fehler kann für gewöhnlich ignoriert werden.
`TOO MANY LOCKS`	Ein internes Problem ist aufgetreten. Wenden Sie sich an Ihren Systemanbieter.
`XMV ERROR`	Ein Problem mit einer Datei oder einem Verzeichnis ist aufgetreten. Das Spool-Verzeichnis ist die wahrscheinliche Ursache, da die Modi der Ziele geprüft werden sollten, bevor versucht wurde, diesen Prozess auszuführen.
`CAN'T FORK`	Ein Versuch, einen `fork`- und `exec`-Vorgang auszuführen, ist fehlgeschlagenen. Der aktuelle Job sollte noch vorhanden sein, und es wird später versucht, ihn erneut auszuführen (`uuxqt`). Es ist keine Aktion erforderlich.

UUCP-STATUS-Fehlermeldungen

In der folgenden Tabelle sind die häufigsten STATUS-Fehlermeldungen aufgeführt.

TABELLE 26–8 UUCP-STATUS-Meldungen

Fehlermeldung	Beschreibung/Aktion
`OK`	Der Status ist akzeptabel.
`NO DEVICES AVAILABLE`	Es steht derzeit kein Gerät für den Aufruf zur Verfügung. Prüfen Sie, ob für das betreffende System ein gültiges Gerät in der `Devices`-Datei vorhanden ist. Prüfen Sie die `Systems`-Datei des Geräts, dass zum Aufrufen des Systems verwendet werden soll.
`WRONG TIME TO CALL`	Ein System wurde zu einer Zeit aufgerufen, die nicht in der `Systems`-Datei definiert ist.

TABELLE 26–8 UUCP-STATUS-Meldungen *(Fortsetzung)*

Fehlermeldung	Beschreibung/Aktion
`TALKING`	Selbsterklärend.
`LOGIN FAILED`	Die Anmeldung des betreffenden Rechners ist fehlgeschlagenen. Die Ursache kann eine falsche Anmeldung oder ein falsches Passwort sein, ein langsamer Rechner oder ein Fehler bei der Ausführung des Dialer-Token-Paar-Skripts.
`CONVERSATION FAILED`	Der Dialog ist nach erfolgreichem Start fehlgeschlagen. Dieser Fehler weist normalerweise darauf hin, dass einer der Teilnehmer ausgefallen ist, das Programm abgebrochen wurde oder die Leitung (Verbindung) unterbrochen wurde.
`DIAL FAILED`	Der Remote-Rechner antwortet nicht. Die Ursache kann ein fehlerhafter Dialer oder eine falsche Telefonnummer sein.
`BAD LOGIN/MACHINE COMBINATION`	Der Rechner hat den Aufruf mit einer Anmeldung bzw. einem Rechnernamen durchgeführt, der nicht mit den Angaben in der `Permissions`-Datei übereinstimmt. Dieser Fehler kann ein Täuschungsversuch sein.
`DEVICE LOCKED`	Das aufrufende Gerät, das verwendet werden soll, ist derzeit gesperrt und wird von einem anderen Prozess verwendet.
`ASSERT ERROR`	Ein `ASSERT`-Fehler ist aufgetreten. Suchen Sie den Fehler in der `/var/uucp/.Admin/errors` -Datei, und informieren Sie sich im Abschnitt „UUCP-ASSERT-Fehlermeldungen“ auf Seite 635.
`SYSTEM NOT IN Systems FILE`	Das System ist nicht in der `Systems`-Datei angegeben.
`CAN'T ACCESS DEVICE`	Das betreffende Gerät ist nicht vorhanden, oder die Modi sind ungültig. Prüfen Sie die entsprechenden Einträge in den `Systems` - und `Devices`-Dateien.
`DEVICE FAILED`	Das Gerät konnte nicht aktiviert werden.
`WRONG MACHINE NAME`	Der aufgerufene Rechner gibt nicht den erwarteten Namen zurück.
`CALLBACK REQUIRED`	Es wird verlangt, dass der aufgerufene Rechner Ihren Rechner aufruft.
`REMOTE HAS A LCK FILE FOR ME`	Der Remote-Rechner hat eine `LCK`-Datei für Ihren Rechner. Der Remote-Rechner kann eventuell gerade versuchen, Ihren Rechner aufzurufen. Wenn der Remote-Rechner eine ältere UUCP-Version verwendet, kann der Prozess, über den mit Ihrem Rechner kommuniziert wurde, fehlgeschlagen sein, wodurch die `LCK`-Datei verlassen wurde. Wenn der Remote-Rechner die neue UUCP-Version verwendet und nicht mit Ihrem Rechner kommuniziert, ist der Prozess, der eine `LCK`-Datei verwendet, hängen geblieben.
`REMOTE DOES NOT KNOW ME`	Der Knotenname Ihres Rechners ist nicht in der `Systems`-Datei des Remote-Rechners enthalten.
`REMOTE REJECT AFTER LOGIN`	Die von Ihrem Rechner verwendeten Anmeldeinformationen stimmen nicht mit den vom Remote-Rechner erwarteten Informationen überein.
`REMOTE REJECT, UNKNOWN MESSAGE`	Der Remote-Rechner hat die Kommunikation mit Ihrem Rechner aus einem unbekannten Grund abgelehnt. Eventuell wird auf dem Remote-Rechner keine standardmäßige UUCP-Version ausgeführt.

TABELLE 26–8 UUCP-STATUS-Meldungen *(Fortsetzung)*

Fehlermeldung	Beschreibung/Aktion
`STARTUP FAILED`	Die Anmeldung wurde erfolgreich durchgeführt, aber der anfängliche Quittierungsaustausch ist fehlgeschlagenen.
`CALLER SCRIPT FAILED`	Dieser Fehler ist derselbe wie `DIAL FAILED`. Wenn dieser Fehler jedoch häufig auftritt, könnte das Skript des aufrufenden Programms in der `Dialers`-Datei die Ursache sein. Verwenden Sie `Uutry` , um dies zu prüfen.

Nummerische UUCP-Fehlermeldungen

In der nachstehenden Tabelle werden die Beendigungscodenummern der Fehlermeldungen aufgeführt, die durch die `/usr/include/sysexits.h`-Datei generiert werden. Nicht alle Codenummern werden derzeit von `uucp` verwendet.

TABELLE 26–9 Nummerische UUCP-Fehlermeldungen

Nummer der Fehlermeldung	Beschreibung	Bedeutung
`64`	Basiswert für Fehlermeldungen	Fehlermeldungen beginnen mit diesem Wert.
`64`	Fehler durch Verwendung der Befehlszeile	Ein falscher Befehl wurde verwendet, beispielsweise ein Befehl mit einer falschen Anzahl von Argumenten, einem falschen Flag oder einer falschen Syntax.
`65`	Datenformatfehler	Die eingegangenen Daten waren in irgendeiner Form fehlerhaft. Dieses Datenformat sollte nur für Benutzerdaten verwendet werden, nicht aber für Systemdateien.
`66`	Keine Eingabe	Eine Eingabedatei, nicht aber eine Systemdatei, ist nicht vorhanden oder nicht lesbar. Dieses Problem kann auch mit Fehlermeldungen wie "No message" in Verbindung stehen, die an einen Mailer gesendet werden.
`67`	Unbekannte Adresse	Der angegeben Benutzer ist nicht vorhanden. Dieser Fehler kann sich auf Mailadressen oder Remote-Anmeldungen beziehen.
`68`	Unbekannter Hostname	Der Host ist nicht vorhanden. Dieser Fehler bezieht sich auf Mailadressen oder Netzwerkanforderungen.
`69`	Service nicht verfügbar	Ein Service ist nicht verfügbar. Dieser Fehler kann auftreten, wenn ein Unterstützungsprogramm oder eine Datei nicht vorhanden ist. Diese Meldung kann einfach auch nur bedeuten, dass etwas nicht funktioniert und die Ursache derzeit nicht ermittelt werden kann.
`70`	Interner Softwarefehler	Ein interner Softwarefehler wurde erkannt. Dieser Fehler sollte, sofern möglich, auf nicht betriebssystembezogene Fehler eingegrenzt werden.

TABELLE 26–9 Nummerische UUCP-Fehlermeldungen *(Fortsetzung)*

Nummer der Fehlermeldung	Beschreibung	Bedeutung
71	Systemfehler	Ein Betriebssystemfehler wurde erkannt. Dieser Fehler bezieht sich auf Zustände wie "fork nicht möglich" und "Pipe kann nicht erstellt werden". Diese Fehlermeldung enthält beispielsweise eine `getuid`-Rückgabe eines Benutzers, der nicht in der `passwd`-Datei vorhanden ist.
72	Eine wichtige Betriebssystemdatei fehlt	Ein Systemdatei wie beispielsweise `/etc/passwd` oder `/var/admin/utmpx` ist nicht vorhanden, kann nicht geöffnet werden oder weist einen Fehler auf (beispielsweise einen Syntaxfehler).
73	Ausgabedatei kann nicht erstellt werden	Eine benutzerdefinierte Ausgabedatei kann nicht erstellt werden.
74	Ein-/Ausgabefehler	Während der Eingabe/Ausgabe über eine Datei ist ein Fehler aufgetreten.
75	Temporärer Fehler. Der Benutzer wird zur Wiederholung des Vorgangs aufgefordert.	Ein temporärer Ausfall, der kein wirklicher Fehler ist. In `sendmail` bedeutet dies beispielsweise, dass ein Mailer keine Verbindung herstellen konnte und der Versuch zu einem späteren Zeitpunkt wiederholt werden sollte.
76	Remote-Fehler im Protokoll	Das Remote-System hat einen Vorgang gemeldet, der während eines Protokollaustauschs nicht durchgeführt werden konnte.
77	Zugriff verweigert	Sie haben keine ausreichende Berechtigung, um den Vorgang auszuführen. Diese Meldung bezieht sich nicht auf Dateisystemprobleme, bei denen `NOINPUT` oder `CANTCREAT` verwendet werden sollte, sondern auf Berechtigungen auf hoher Ebene. Beispielsweise wird diese Meldung von `kre` verwendet, um das Versenden von Mails durch Studenten zu beschränken.
78	Konfigurationsfehler	Das System hat einen Konfigurationsfehler erkannt.
79	Eintrag nicht gefunden	Ein Eintrag wurde nicht gefunden.
79	Maximaler gelisteter Wert	Höchster Wert für Fehlermeldungen

TEIL VI

Arbeiten mit Remote-Systemen – Themen

Dieser Abschnitt enthält Verfahren zum Verwalten eines FTP-Servers und für den Zugriff auf Remote-Systeme in der Solaris-Umgebung.

◆ ◆ ◆ KAPITEL 27

Arbeiten mit Remote-Systemen (Übersicht)

Dieser Abschnitt enthält Informationen zum Arbeiten mit Remote-Dateien.

- „Was ist ein FTP-Server?“ auf Seite 643
- „Was ist ein Remote-System?“ auf Seite 643
- „Aktuelle Änderungen am FTP-Service“ auf Seite 644

Was ist ein FTP-Server?

Der FTP-Server basiert auf wu-ftpd. wu-ftpd wurde ursprünglich an der Washington University in Saint Louis entwickelt und wird zur Übertragung von großen Datenmengen über das Internet eingesetzt. wu-ftpd ist der bevorzugte Standard für große FTP-Standorte. Informationen zu den Lizenzbedingungen finden Sie unter `/var/sadm/pkg/SUNWftpu/install/copyright`.

Was ist ein Remote-System?

Im Zusammenhang mit den in diesem Kapitel beschriebenen Verfahren handelt es sich bei einem *Remote-System* um eine Workstation oder einen Server, der über ein physisches Netzwerk mit dem lokalen System verbunden und für die TCP/IP-Kommunikation konfiguriert ist.

Bei Systemen, auf denen ein Solaris ausgeführt wird, erfolgt die Einrichtung der TCP/IP-Konfiguration automatisch während des Systemstarts. Weitere Informationen finden Sie im *Systemverwaltungshandbuch: IP Services*.

Aktuelle Änderungen am FTP-Service

Frühere Versionen enthielten mehrere Änderungen am FTP-Service. Zu diesen Änderungen zählen Verbesserungen des FTP-Servers sowie Änderungen an den `ftpcount` -, `ftpwho`- und `ftp`-Befehlen.

Durch die Verbesserungen des FTP-Servers werden die Skalierbarkeit und die Übertragungprotokollierung optimiert. Eine Beschreibung dieser Optionen finden Sie unter „Konfigurationshilfe für Standorte mit hoher Auslastung“ auf Seite 676 und auf der Manpage `ftpaccess(4)`. Insbesondere handelt es sich um folgende Verbesserungen:

- Die Funktion `sendfile()` wird für binäre Download-Vorgänge verwendet.
- Die Datei `ftpaccess` bietet Unterstützung für neue Funktionen.
  - `flush-wait` steuert das Verhalten am Ende eines Downloads oder einer Verzeichnisauflistung.
  - `ipcos` dient zum Festlegen der IP-Serviceklasse für die Steuer- oder Datenverbindung.
  - `passive ports` kann so konfiguriert werden, dass der Kernel den TCP-Port auswählt, an dem eine Überwachung stattfindet.
  - `quota-info` dient zum Abrufen von Kontingentinformationen.
  - `recvbuf` dient zum Festlegen die Größe des Empfangspuffers (Upload) für binäre Übertragungen.
  - `rhostlookup` erlaubt bzw. verhindert die Abfrage des Remote-Hostnamens.
  - `sendbuf` dient zum Festlegen der Größe des Sendepuffers (Download) für binäre Übertragungen.
  - `xferlog` dient zum Anpassen des Formats für den Eintrag im Übertragungsprotokoll.
- Die Option `-4` sorgt dafür, dass der FTP-Server einen IPv4-Socket nur dann auf Verbindungen überwacht, wenn er im Einzelbetriebsmodus ausgeführt wird.

Außerdem bieten `ftpcount` und `ftpwho` jetzt Unterstützung für die Option `-v`, mit deren Hilfe Benutzerzählungen und Prozessinformationen für FTP-Serverklassen angezeigt werden, die in `ftpaccess`-Dateien für virtuelle Hosts definiert sind. Weitere Informationen finden Sie auf den Manpages `ftpcount(1)` und `ftpwho(1)`.

Der FTP-Client und der FTP-Server unterstützen jetzt Kerberos. Weitere Informationen finden Sie auf der Manpage `ftp(4)` und unter „Kerberos-Benutzerbefehle“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

Der `ftp`-Befehl wurde geändert. Ein mit einem Solaris FTP-Server verbundener Solaris FTP-Client listet standardmäßig sowohl Verzeichnisse als auch einfache Dateien auf, wenn er den Befehl `ls` erhält. Wenn der FTP-Server nicht im Betriebssystem Solaris ausgeführt wird, werden möglicherweise keine Verzeichnisse aufgelistet. Damit sich Solaris während des Aufbaus einer Verbindung mit anderen Servern (d. h. keinen Solaris-FTP-Servern)

standardmäßig verhält, kann die Datei `/etc/default/ftp` auf den einzelnen Solaris-Clients entsprechend bearbeitet werden. Um die Änderung für einzelne Benutzer vorzunehmen, kann die Umgebungsvariable `FTP_LS_SENDS_NLST` auf `yes` gesetzt werden. Weitere Informationen finden Sie auf der Manpage `ftp(4)`.

Der `ftpd`-Dämon wird von der Service Management Facility verwaltet. Administrative Maßnahmen an diesem Service, beispielsweise Aktivieren, Deaktivieren oder Neustarten können mithilfe des Befehls `svcadm` vorgenommen werden. Der Service-Status aller Dämonen kann mithilfe des Befehls `svcs` abgefragt werden. Eine Übersicht zur Service Management Facility finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*.

◆ ◆ ◆ KAPITEL 28

Verwalten des FTP-Servers (Aufgaben)

In diesem Kapitel werden Aufgaben behandelt, die in der nachstehenden Tabelle beschrieben werden und dazu dienen, einen FTP-Server einzurichten und zu verwalten.

- „Verwalten des FTP-Servers (Übersicht der Schritte)“ auf Seite 647
- „Steuern des FTP-Serverzugriffs“ auf Seite 649
- „Einrichten der Anmeldung für den FTP-Server“ auf Seite 655
- „Anpassen von Meldungsdateien“ auf Seite 659
- „Steuern des Zugriffs auf Dateien auf dem FTP-Server“ auf Seite 663
- „Steuern von Uploads und Downloads auf dem FTP-Server“ auf Seite 664
- „Virtuelles Hosting“ auf Seite 667
- „Automatisches Starten des FTP-Servers“ auf Seite 671
- „Abschalten des FTP-Servers“ auf Seite 673
- „Beheben von FTP-Serverproblemen“ auf Seite 674
- „Konfigurationshilfe für Standorte mit hoher Auslastung“ auf Seite 676

Verwalten des FTP-Servers (Übersicht der Schritte)

TABELLE 28–1 Übersicht der Schritte: Verwalten des FTP-Servers

Aufgabe	Beschreibung	Siehe
Konfigurieren des Zugriffs auf den FTP-Server	Verwenden Sie die Dateien `ftpaccess`, `ftpusers` und `ftphosts` im Verzeichnis `/etc/ftpd`, um den Zugriff auf den FTP-Server einzurichten oder zu beschränken.	„So beschränken Sie Benutzeranmeldungen“ auf Seite 650 „So legen Sie die Anzahl von ungültigen Anmeldeversuchen fest“ auf Seite 652 „Wie bestimmten Benutzern der FTP-Serverzugriff verwehrt wird“ auf Seite 653 „So beschränken Sie den Zugriff auf den standardmäßigen FTP-Server“ auf Seite 654 „So definieren Sie FTP-Serverklassen“ auf Seite 649

TABELLE 28–1 Übersicht der Schritte: Verwalten des FTP-Servers *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Einrichten der Anmeldung für den FTP-Server	Richten Sie Anmeldungskonten für authentische Benutzer, Gastbenutzer und anonyme Benutzer ein.	„So richten Sie den Zugriff für authentische FTP-Benutzer ein“ auf Seite 656 „So richten Sie den Zugriff für FTP-Gastbenutzer ein“ auf Seite 656 „So richten Sie den Zugriff für anonyme FTP-Benutzer ein“ auf Seite 658 „So richten Sie die `/etc/shells`-Datei ein“ auf Seite 658
Anpassen von Meldungsdateien	Bearbeiten Sie die `/etc/ftpd/ftpaccess`-Datei, um den FTP-Server zu konfigurieren, damit dieser ereignisbezogene Meldungen an den FTP-Client zurückgibt.	„So passen Sie Meldungsdateien an“ auf Seite 659 „So erstellen Sie Meldungen, die an Benutzer gesendet werden“ auf Seite 660 „So konfigurieren Sie die README-Option“ auf Seite 661
Konfigurieren des Zugriffs auf Dateien auf dem FTP-Server	Verwenden Sie die `/etc/ftpd/ftpaccess`-Datei, um Klassen von Benutzern anzugeben, denen erlaubt ist, bestimmte Befehle auszuführen oder Dateien vom FTP-Server herunterzuladen oder auf diesen hochzuladen.	„So konfigurieren Sie die DA-Erkennung für DFÜ-Netzwerke“ auf Seite 254 „Steuern von Uploads und Downloads auf dem FTP-Server“ auf Seite 664
Aktivieren des limitierten oder kompletten virtuellen Hosting	Verwenden Sie die `/etc/ftpd/ftpaccess`-Datei, um den FTP-Server zu konfigurieren, damit mehrere Domains auf demselben Rechner unterstützt werden.	„So aktivieren Sie das limitierte virtuelle Hosting“ auf Seite 668 „So aktivieren Sie komplettes virtuelles Hosting“ auf Seite 669
Starten des FTP-Servers	Ändern Sie die Serviceeigenschaften, um den FTP-Server im `nowait`-Modus, im Einzelbetriebsmodus oder im Vordergrundmodus zu starten.	„So starten Sie einen FTP-Server mithilfe von SMF“ auf Seite 671 „So starten Sie einen eigenständigen FTP-Server im Hintergrund“ auf Seite 672 „So starten Sie einen eigenständigen FTP-Server im Vordergrund“ auf Seite 673
Abschalten des FTP-Servers	Verwenden Sie die `/etc/ftpd/ftpaccess`-Datei, und führen Sie den Befehl `ftpshut` aus, um den FTP-Server abzuschalten.	„Abschalten des FTP-Servers“ auf Seite 673

TABELLE 28–1 Übersicht der Schritte: Verwalten des FTP-Servers *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Beheben einiger allgemeiner FTP-Serverprobleme	Prüfen Sie `syslogd`, und verwenden Sie `greeting text` und `Protokollierungsbefehle`, um FTP-Serverprobleme zu beheben.	„So prüfen Sie `syslogd` auf FTP-Servermeldungen“ auf Seite 675 „So verwenden Sie `greeting text`, um `ftpaccess` zu prüfen“ auf Seite 675 „So stellen Sie fest, welche Befehle von FTP-Benutzern ausgeführt wurden“ auf Seite 676

Steuern des FTP-Serverzugriffs

Sie können die folgenden Konfigurationsdateien im Verzeichnis `/etc/ftpd` verwenden, um den Zugriff auf den FTP-Server zu steuern.

- `ftpusers` wird verwendet, um Benutzer aufzulisten, denen der Zugriff auf den FTP-Server verwehrt wird.
- `ftphosts` wird verwendet, um die Anmeldung von verschiedenen Hosts bei verschiedenen Konten des FTP-Servers zu gestatten oder abzulehnen.
- `ftpaccess` ist die FTP-Hauptkonfigurationsdatei . Der FTP-Server liest die `/etc/ftpd/ftpaccess` -Datei nur dann, wenn er mit der Option `-a` aufgerufen wird. Wenn die `ftpaccess`-Datei verwendet wird, müssen alle Benutzer zu einer Klasse gehören, damit Zugriff auf den FTP-Server gewährt werden kann. Sie können viele `ftpaccess`-Anweisungen angeben, die ausschließlich für eine bestimmte Klasse gelten.

  Weitere Informationen finden Sie unter `ftpusers(4)`, `ftphosts(4)` und `ftpaccess(4)`.

Hinweis – Alle Zeilen in FTP-Serverkonfigurationsdateien, die mit einem Nummernzeichen (#) beginnen, werden als Kommentare behandelt.

▼ So definieren Sie FTP-Serverklassen

Um sich bei einem FTP-Server anmelden zu können, müssen Benutzer zu einer Klasse gehören, wenn die `ftpaccess`-Datei verwendet wird. Um die `class`-Anweisung in die `ftpaccess`-Datei einzufügen, geben Sie die *class* name, *typelist* der Benutzer an, die berechtigt sind, den Zugriff über einen bestimmten Host durchzuführen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie die entsprechenden Einträge für anonyme Benutzer, Gastbenutzer und authentische Benutzer in die `ftpaccess`-Datei ein.

`class` *class typelist addrglob*`[`*addrglob...*`]`

`class` Schlüsselwort, das zum Definieren von FTP-Benutzern verwendet wird

class Ein Name, der durch das Schlüsselwort `class` definiert wird. Jede Anmeldung wird mit einer Liste von definierten Klassen abgeglichen. Der angemeldete Benutzer wird als zugehörig zu der Klasse betrachtet, die als erste abgeglichen wurde.

typelist Eine durch Komma getrennte Liste der Schlüsselwörter zum Abgleichen der drei Benutzertypen `anonymous`, `guest` und `real` (anonymer Benutzer, Gastbenutzer, authentischer Benutzer)

addrglob Ein mit mithilfe des Globbing erstellter Domainname oder eine mithilfe des Globbing erstellte nummerische Adresse. Der Eintrag *addrglob* kann auch der Name einer Datei sein, die mit einem Schrägstrich (/) beginnt und weitere Address-Globs enthält: `address:netmask` oder `address/cidr`.

Es folgen einige Beispiele für Adressen, die mithilfe des Globbing erstellt wurden:

- Nummerische IPv4-Adresse: **`10.1.2.3`**
- Mithilfe des Globbing erstellter Domainname **`*.provider.com`**
- Mithilfe des Globbing erstellte nummerische IPv4-Adresse **`10.1.2.*`**
- Nummerische IPv4 Adresse:Netzmaske **`10.1.2.0:255.255.255.0`**
- Nummerische IPv4-Adresse/CIDR **`10.1.2.0/24`**
- Nummerische IPv6-Adresse: **`2000::56:789:21ff:fe8f:ba98`**
- Nummerische IPv6-Adresse/CIDR: **`2000::56:789:21ff:fe8f:ba98/120`**

Beispiel 28–1 Definieren von FTP-Serverklassen

```
class  local  real,guest,anonymous *.provider.com
class  remote real,guest,anonymous *
```

Im vorangegangenen Beispiel wird die Klasse `local` als ein Benutzer des Typs `real`, `guest` oder `anonymous` definiert, der sich über `*.provider.com` anmeldet. In der letzten Zeile wird `remote` als ein Benutzer definiert, der sich von einer beliebigen Stelle aus anmeldet, nicht aber über `*.provider.com`.

▼ So beschränken Sie Benutzeranmeldungen

Sie können die Anzahl von gleichzeitigen Anmeldungen der Benutzer von bestimmten Klassen durch Anweisungen beschränken, die in der `ftpaccess`-Datei definiert sind. Jede Anmeldungsbeschränkung enthält den Namen einer Klasse, eine UUCP-basierte Liste der Wochentage und eine Meldungsdatei, die angezeigt wird, wenn das definierte Limit überschritten ist.

Gehen Sie wie folgt vor, um Beschränkungen für Benutzeranmeldungen festzulegen:

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:**

`limit` *class n times* [*message-file*]

`limit`	Schlüsselwort, das verwendet wird, um die Häufigkeit gleichzeitiger Anmeldungen einer bestimmten Anzahl von Benutzern einer definierten Klasse zu bestimmten Zeiten zu beschränken
Klasse	Ein Name, der durch das Schlüsselwort `class` definiert wird. Jede Anmeldung wird mit einer Liste von definierten Klassen abgeglichen. Der angemeldete Benutzer wird als zugehörig zu der Klasse betrachtet, die als erste abgeglichen wurde.
n	Anzahl von Benutzern
Häufigkeit	Wochentag und Uhrzeit, zu der die Klasse verbunden werden kann. Verwenden Sie `Any` für einen beliebigen Tag.
Meldungsdatei	Meldungsdatei, die angezeigt wird, wenn einem Benutzer der Zugriff verweigert wird

Beispiel 28–2 Beschränken von Benutzeranmeldungen

```
limit   anon     50  Wk0800-1800        /etc/ftpd/ftpmsg.deny
limit   anon    100  Any                /etc/ftpd/ftpmsg.deny
limit   guest   100  Any                /etc/ftpd/ftpmsg.deny
```

Die erste Zeile des vorangegangenen Beispiels zeigt ein Limit von 50 gleichzeitigen Anmeldungen, die Benutzern der Klasse `anon` innerhalb der Wochenarbeitszeit erlaubt sind. In der zweiten Zeile werden den Benutzern der Klasse `anon` 100 gleichzeitige Anmeldungen außerhalb der Arbeitszeit erlaubt. Die letzte Zeile zeigt ein Limit von 100 `guest` -Anmeldungen, die jederzeit durchgeführt werden können. Informationen zur Festlegung der Tages- und Zeitparameter finden Sie unter `ftpaccess(4)`.

Das Beispiel zeigt zudem, dass der Inhalt der Datei `/etc/ftpd/ftpmsg.deny` zurückgegeben wird, wenn ein bestimmtes Anmeldungslimit erreicht ist – sofern `ftpmsg.deny` vorhanden ist. Informationen, wie der `/usr/sbin/ftpcount` -Befehl zu verwenden ist, um die Anzahl und das Limit der Anmeldungen für jede Klasse von Benutzern anzuzeigen, die zu einer bestimmten Zeit angemeldet sind, finden Sie unter `ftpcount(1)`.

Benutzern ist es erlaubt, sich beim FTP-Server anzumelden, es sei denn, ein bestimmtes Limit wurde erreicht. Anonyme Benutzer werden als `ftp`-Benutzer angemeldet. Authentische Benutzer werden mit ihrem eigenen Benutzernamen angemeldet, und Gastbenutzer werden als authentische Benutzer mit einer `chroot`-Umgebung angemeldet, wodurch der Zugriff beschränkt wird.

Informationen, wie der `/usr/sbin/ftpwho`-Befehl verwendet wird, um die Identität der beim FTP-Server angemeldeten Benutzer zu prüfen, finden Sie unter `ftpwho(1)`.

▼ So legen Sie die Anzahl von ungültigen Anmeldeversuchen fest

Wenn eine Anmeldung beim FTP-Server aufgrund eines Problems wie beispielsweise falscher Schreibweise fehlschlägt, wird die Anmeldung normalerweise wiederholt. Dem Benutzer ist eine bestimmte Anzahl von aufeinanderfolgenden Anmeldeversuchen gestattet, bevor eine Meldung in der `syslog`-Datei protokolliert wird. An diesem Punkt wird der Benutzer getrennt. Anhand des nächsten Verfahrens können Sie ein Limit für Anmeldeversuche festlegen.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:

```
loginfails n
```

loginfails	Schlüsselwort, mit dem festgelegt wird, wie viele Anmeldeversuche fehlschlagen können, bevor die FTP-Verbindung getrennt wird
n	Anzahl von Anmeldeversuchen, die fehlschlagen können

Beispiel 28–3 Festlegen der Anzahl von ungültigen Anmeldeversuchen

```
loginfails 10
```

Das vorangegangene Beispiel zeigt, dass der Benutzer nach 10 fehlgeschlagenen Anmeldeversuchen vom FTP-Server getrennt wird.

▼ Wie bestimmten Benutzern der FTP-Serverzugriff verwehrt wird

In der `/etc/ftpd/ftpusers`-Datei sind die Namen von Benutzern aufgelistet, denen nicht gestattet ist, sich beim FTP-Server anzumelden. Wenn ein Anmeldeversuch gemacht wird, prüft der FTP-Server die `/etc/ftpd/ftpusers`-Datei, um festzustellen, ob dem Benutzer der Zugriff erlaubt ist. Wenn der Name des Benutzers nicht in der Datei gefunden wird, sucht der Server in der `/etc/ftpusers`-Datei.

Wenn der Name des Benutzers in `/etc/ftpusers` abgeglichen werden kann, wird eine `syslogd`-Meldung ausgegeben, in der darauf hingewiesen wird, dass die Übereinstimmung in einer veralteten Datei gefunden wurde. Auch wird in der Meldung die Verwendung von `/etc/ftpd/ftpusers` anstelle von `/etc/ftpusers` empfohlen.

Hinweis – In dieser Version wird die `/etc/ftpusers`-Datei nicht mehr verwendet. Ist die `/etc/ftpusers`-Datei vorhanden, wenn der FTP-Server installiert wird, wird die Datei in die `/etc/ftpd/ftpusers` -Datei verschoben.

Weitere Informationen finden Sie auf den Manpages `syslogd(1M)`, `in.ftpd(1M)` und `ftpusers(4)`

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Fügen Sie für Benutzer, denen die Anmeldung beim FTP-Server nicht erlaubt ist, entsprechende Einträge in die `/etc/ftpd/ftpusers`-Datei ein.**

Beispiel 28–4 Verweigern des Zugriffs auf den FTP-Server

```
root
daemon
bin
sys
adm
lp
uccp
nuucp
listen
nobody
noaccess
nobody4
```

Das vorangegangene Beispiel zeigt typische Einträge in der `ftpusers`-Datei. Die Benutzernamen stimmen mit den Einträgen in `/etc/passwd` überein. In der Liste sind `root` und andere administrative und systemspezifische Identitäten enthalten.

Der Root-Eintrag ist aus Sicherheitsgründen in der `ftpusers`-Datei enthalten. Gemäß der standardmäßigen Sicherheitsrichtlinie ist eine Remote-Anmeldungen als Root-Benutzer nicht gestattet. Diese Richtlinie gilt auch für den Standardwert, der als CONSOLE-Eintrag in `/etc/default/loginfile` definiert ist. Siehe dazu `login(1)`.

▼ So beschränken Sie den Zugriff auf den standardmäßigen FTP-Server

Zusätzlich zu den oben genannten Sicherheitsmaßnahmen können Sie explizite Einträge in die `ftpaccess`-Datei einfügen, um den Zugriff auf den FTP-Server zu beschränken.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:

a. Allen Benutzern wird standardmäßig der Zugriff auf den standardmäßigen (nicht virtuellen) FTP-Server gewährt. Um bestimmten (nicht `anonym` angemeldeten) Benutzern den Zugriff zu verwehren, fügen Sie folgenden Eintrag ein:

`defaultserver deny` *username* `[`*username...*`]`

`defaultserver`	Schlüsselwort, das verwendet wird, um den nicht virtuellen Server zu identifizieren, auf den der Zugriff erlaubt oder verwehrt werden kann
username	Anmeldename eines Benutzers mit beschränktem Zugriff auf den `defaultserver`

b. Um Benutzern Zugriff zu gewähren, die nicht auf der `deny`-Zeile aufgeführt sind, fügen Sie die folgende Zeile ein:

`defaultserver allow` *username* `[`*username...*`]`

c. Um anonymen Benutzern den Zugriff zu verwehren, fügen Sie die folgende Zeile ein:

```
defaultserver private
```

Beispiel 28–5 Beschränken des Zugriffs auf den standardmäßigen FTP-Server

```
defaultserver deny *
defaultserver allow username
```

Das vorangegangene Beispiel zeigt, dass der FTP-Server allen Benutzern außer `anon`-Benutzern und den auf der `allow`-Zeile aufgeführten Benutzern den Zugriff verwehrt.

Sie können auch die `ftphosts`-Datei verwenden, um zu verhindern, dass über verschiedene Hosts auf Anmeldungskonten zugegriffen wird. Weitere Informationen finden Sie unter `ftphosts(4)`.

Einrichten der Anmeldung für den FTP-Server

Um auf einen FTP-Server zugreifen zu können, müssen Sie sich zunächst anmelden. Der FTP-Server unterstützt drei Arten von Benutzeranmeldungskonten für authentische Benutzer, Gastbenutzer und anonyme Benutzer.

- Authentische Benutzer haben Konten, mit deren Hilfe Terminalsitzungen auf Systemen eingerichtet werden können, auf denen der FTP-Server ausgeführt wird. Entsprechend den Verzeichnis- und Dateizugriffsberechtigungen ist die gesamte Festplattenstruktur für authentische Benutzer sichtbar.
- Gastbenutzer benötigen Konten, um sich beim FTP-Server anzumelden. Jedes Gastkonto wird mit einem Benutzernamen und einem Passwort eingerichtet. Aktive Anmelde-Shells werden Gastbenutzern nicht zugänglich gemacht, um zu verhindern, dass Terminalsitzungen durchgeführt werden. Bei der Anmeldung führt der FTP-Server einen `chroot(2)`-Vorgang durch, um die Sicht eines Gastbenutzer auf die Festplattenstruktur des Servers zu beschränken.

  Hinweis – Anmelde-Shells für authentische und Gastbenutzer müssen in der Datei `/etc/shells` aufgelistet sein, damit auf den FTP-Server zugegriffen werden kann.

- Anonyme Benutzer melden sich beim FTP-Server an, indem sie entweder `ftp` oder `anonymous` als Benutzername angeben. Üblicherweise geben anonyme Benutzer eine E-Mail-Adresse an, wenn sie zur Eingabe eines Passworts aufgefordert werden.

  Bei der Anmeldung führt der FTP-Server einen `chroot(2)`-Vorgang durch, um die Sicht eines anonymen Benutzers auf die Festplattenstruktur des Servers zu beschränken. Ein einzelner Dateibereich wird von allen anonymen Benutzern genutzt, während separate Bereiche für jeden Gastbenutzer bereitgestellt werden können.

Authentische und Gastbenutzer melden sich über individuelle Konten mit Passwörtern an, die nur einer einzelnen Person bekannt sind. Anonyme Benutzer melden sich bei einem allgemein bekannten Konto an, das potentiell allen Benutzern zur Verfügung steht. Meist sind umfangreiche Dateitransfers auf die Verwendung von anonymen Konten zurückzuführen.

▼ So richten Sie den Zugriff für authentische FTP-Benutzer ein

Gehen Sie wie folgt vor, um authentischen Benutzern den Zugriff auf den FTP-Server zu ermöglichen:

1 **Stellen Sie sicher, dass der Benutzer ein Konto hat, das mit einem Benutzernamen und einem Passwort eingerichtet ist, die zur Durchführung einer Terminalsitzung verwendet werden können.**

Weitere Informationen finden Sie in Kapitel 4, „Managing User Accounts and Groups (Overview)“ in *System Administration Guide: Basic Administration*.

2 **Stellen Sie sicher, dass der authentische Benutzer zu einer Klasse in der `ftpaccess`-Datei gehört.**

Informationen zu den Benutzerklassen, die in der `ftpaccess`-Datei definiert sind, finden Sie unter „So definieren Sie FTP-Serverklassen“ auf Seite 649.

3 **Stellen Sie sicher, dass die Anmelde-Shell des Benutzers in der `/etc/shells`-Datei aufgelistet ist.**

▼ So richten Sie den Zugriff für FTP-Gastbenutzer ein

Das `ftpconfig`-Skript wird verwendet, um alle benötigten Systemdateien in das Home-Verzeichnis zu kopieren. Wenn der Gastbenutzer und das Home-Verzeichnis des Gastbenutzers bereits vorhanden sind, bewirkt das `ftpconfig`-Skript, dass der Bereich mit den aktuellen Systemdateien aktualisiert wird.

Weitere Informationen finden Sie auf der Manpage `ftpconfig(1M)`

Hinweis – Anders als der Benutzername (`anonymous` oder `ftp`), der für anonymen Benutzer festgelegt ist, sind Benutzernamen für FTP-Benutzer nicht festgelegt. Es kann jeder Name gewählt werden, der als authentischer Benutzername angegeben werden kann.

Gehen Sie wie folgt vor, um einem Gastbenutzer den Zugriff auf den FTP-Server zu ermöglichen:

1 **Verwenden Sie das `useradd`-Skript, um ein Gastbenutzerkonto mit einer Anmelde-Shell von `/bin/true` und einem Home-Verzeichnis von** */root-dir/./home-dir* **zu erstellen.**

Weitere Informationen finden Sie auf der Manpage useradd(1M) und in Kapitel 4, „Managing User Accounts and Groups (Overview)“ in *System Administration Guide: Basic Administration*.

Hinweis – In diesem Verfahren wird **`/home/guests/./guest1`** als Home-Verzeichnisname für einen Benutzer namens `guest1` verwendet.

```
# /usr/sbin/useradd -m -c "Guest FTP" -d \
  /home/guests/./guest1 -s /bin/true guest1
```

2 **Weisen Sie dem Gastkonto ein Passwort zu.**

3 **Fügen Sie einen `guestuser`-Eintrag in die `ftpaccess`-Datei ein.**

```
guestuser guest1
```

Hinweis – Sie können auch die `guestgroup`-Funktion in der `ftpaccess`-Datei verwenden, um Gastbenutzer zu definieren. Durch die `guest-root`-Funktion in `ftpaccess` wird `/./` im Home-Verzeichnispfad des Gastbenutzers nicht mehr benötigt.

---

4 **Stellen Sie sicher, dass der Gastbenutzer zu einer Klasse in der `ftpaccess`-Datei gehört. Weitere Informationen finden Sie unter „So definieren Sie FTP-Serverklassen“ auf Seite 649.**

5 **Verwenden Sie das `ftpconfig`-Skript, um die benötigten Dateien im `chroot`-Bereich zu erstellen.**

```
/usr/sbin/ftpconfig -d /home/guests
```

6 **Stellen Sie sicher, dass `/bin/true` in der `/etc/shells`-Datei aufgelistet ist. Lesen Sie dazu „So richten Sie die `/etc/shells`-Datei ein“ auf Seite 658.**

Beispiel 28–6 Einrichten eines FTP-Servers für Gastbenutzer

In diesem Beispiel wird der FTP-Bereich im `/home/guests`-Verzeichnis eingerichtet.

```
# /usr/sbin/ftpconfig -d /home/guests
Updating directory /home/guests
```

▼ So richten Sie den Zugriff für anonyme FTP-Benutzer ein

Durch das `ftpconfig`-Skript wird das Konto für anonyme Benutzer erstellt, und die benötigten Dateien werden in das Home-Verzeichnis eingefügt.

Weitere Informationen finden Sie auf der Manpage `ftpconfig(1M)`.

Gehen Sie wie folgt vor, um einem anonymen Benutzer den Zugriff auf den FTP-Server zu ermöglichen:

1. **Verwenden Sie das `ftpconfig`-Skript, um das Konto für anonyme Benutzer zu erstellen.**

   `/usr/sbin/ftpconfig` *anonymous-ftp-directory*

2. **Stellen Sie sicher, dass der anonyme Benutzer einer Klasse in der `ftpaccess`-Datei zugewiesen ist.**

   Weitere Informationen finden Sie unter „So definieren Sie FTP-Serverklassen“ auf Seite 649.

Beispiel 28–7 Einrichten des Zugriffs für anonyme FTP-Benutzer

In diesem Beispiel wird der FTP-Bereich im `/home/ftp`-Verzeichnis eingerichtet.

```
# /usr/sbin/ftpconfig /home/ftp
Creating user ftp
Updating directory /home/ftp
```

▼ So richten Sie die `/etc/shells`-Datei ein

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Erstellen Sie die `/etc/shells`-Datei.**

3. **Bearbeiten Sie `/etc/shells`. Fügen Sie den vollständigen Pfad für jede Shell auf einer einzelnen Zeile ein.**

Beispiel 28–8 Erstellen der /etc/shells-Datei

Das folgende Beispiel zeigt eine `/etc/shells`-Datei mit `/bin/true` für FTP-Gastbenutzer:

```
/sbin/sh
/bin/csh
/bin/jsh
/bin/ksh
/bin/remsh
/bin/rksh
/bin/rsh
/bin/sh
/usr/bin/csh
/usr/bin/ksh
/usr/bin/bash
/usr/bin/tcsh
/usr/bin/zsh
/bin/true
```

Anpassen von Meldungsdateien

Sie können den FTP-Server konfigurieren, damit dieser ereignisbezogene Meldungen an den FTP-Client zurückgibt. Es kann eine Begrüßungsmeldung eingerichtet werden, die angezeigt wird, wenn sich ein Benutzer beim FTP-Server anmeldet. Eine andere Meldung kann angezeigt werden, wenn der Benutzer in ein anderes Verzeichnis wechselt.

Neben Klartext können Meldungsdateien ein oder mehrere *magische Cookies* enthalten. Ein magisches Cookie besteht aus einem Prozentzeichen (`%`), dem ein einzelnes Zeichen folgt. Wenn Sie ein Cookie im Meldungstext einbetten, werden die zum Cookie gehörenden Informationen auf dem Bildschirm angezeigt, sobald die Meldungsdatei aufgerufen wird.

Im Meldungstext kann beispielsweise das Cookie `%L` enthalten sein:

```
Welcome to %L!
```

Wenn die Meldung angezeigt wird, wird das magische Cookie `%L` durch den Namen des Servers ersetzt, der durch den `hostname`-Eintrag in der `ftpaccess`-Datei definiert ist. Eine vollständige Liste der unterstützten Meldungs-Cookies finden Sie unter `ftpaccess(4)`.

Hinweis – Wenn der Hostname nicht in der `ftpaccess`-Datei definiert ist, wird der standardmäßige Hostname für den lokalen Rechner verwendet.

▼ So passen Sie Meldungsdateien an

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie nach Bedarf magische Cookies in Ihre Meldungsdatei ein.

Eine Liste der Cookies, die Sie verwenden können, finden Sie unter `ftpaccess(4)`.

Beispiel 28–9 Anpassen von Meldungsdateien

Es folgt ein Beispiel einer Meldungsdatei, die magische Cookies enthält:

```
Welcome to %L -- local time is %T.

You are number %N out of a maximum of %M.
All transfers are logged.

If your FTP client crashes or hangs shortly after login
please try
using a dash (-) as the first character of your password.
This will
turn off the informational messages that may be confusing
your FTP
client.

Please send any comments to %E.
```

▼ So erstellen Sie Meldungen, die an Benutzer gesendet werden

Nachdem sich ein Benutzer angemeldet hat, werden system- oder anwendungsbezogene Meldungen auf dem Bildschirm angezeigt. Die `ftpaccess`-Datei dient zum Auflisten der Ereignisse, mit denen die Ausgabe der entsprechenden `message`-Anweisungen ausgelöst wird.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:

`message` *message-file* `[`*when* `[`*class* ...`]]`

`message`	Schlüsselwort, das verwendet wird, um die Meldungsdatei anzugeben, die angezeigt wird, wenn sich ein Benutzer anmeldet oder den Befehl zum Wechseln in das Arbeitsverzeichnis ausführt
message-file	Name der Meldungsdatei, die angezeigt werden soll
when	Parameter, der mit `login` oder `cwd=` *dir* definiert wird. Siehe das folgende Beispiel.

class Die `class`-Angabe erlaubt, dass die Meldung nur für Benutzer angezeigt wird, die zu einer bestimmten Klasse gehören.

Beispiel 28–10 Erstellen von Meldungen, die an Benutzer gesendet werden

```
message    /etc/ftpd/Welcome    login   anon guest
message    .message    cwd=*
```

Das vorangegangene Beispiel zeigt, dass die Datei `/etc/ftpd/Welcome` angezeigt wird, wenn sich Benutzer der Klasse `anon` oder `guest` anmelden. Auf der zweiten Zeile ist angegeben, dass die `.message`-Datei im aktuellen Arbeitsverzeichnis für alle Benutzer angezeigt wird.

Meldungsdateien werden in Relation zum `chroot`-Verzeichnis für Gastbenutzer und anonyme Benutzer erstellt.

▼ So konfigurieren Sie die README-Option

Wenn zum ersten Mal auf ein Verzeichnis zugegriffen wird, können `README`-Dateien aufgelistet werden. Um die README-Option zu konfigurieren, fügen Sie die folgenden Einträge in die `ftpaccess`-Datei ein.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:

`readme` *message-file* `[when [`*class*`...]]`

`readme` Schlüsselwort, das verwendet wird, um eine Meldungsdatei anzugeben, die geprüft wird, wenn sich ein Benutzer anmeldet oder in das Arbeitsverzeichnis wechselt. Wenn die Meldungsdatei vorhanden ist, wird der Benutzer benachrichtigt und erhält Kenntnis vom Datum, an dem die Datei modifiziert wurde.

message-file Name der Meldungsdatei, die geprüft werden soll

when Parameter, der mit `login` oder `cwd=` *dir* definiert wird. Siehe das folgende Beispiel.

class Mithilfe der `class`-Angabe wird festgelegt, dass die Meldung nur Benutzern angezeigt wird, die zu einer bestimmten Klasse gehören.

Hinweis – Die Schlüsselwörter `greeting` und `banner` können auch verwendet werden, um Meldungen an Benutzer zu senden. Siehe dazu `ftpaccess(4)`.

Beispiel 28–11 Konfigurieren der README-Option

```
readme  README*     login
readme  README*     cwd=*
```

Das vorangegangene Beispiel zeigt, dass Dateien, die mit `README*` übereinstimmen, bei der Anmeldung oder bei einem Verzeichniswechsel aufgelistet werden. Es folgt ein Beispiel einer Anmeldung, die auf den im Beispiel verwendeten Einstellungen basiert.

```
% ftp earth
Connected to earth.
220 earth FTP server ready.
Name (earth:rimmer): ftp
331 Guest login ok, send your complete e-mail address as password.
Password:
230-
230-Welcome to earth -- local time is Thu Jul 15 16:13:24
1999.
230-
230-You are number 1 out of a maximum of 10.
230-All transfers are logged.
230-
230-If your FTP client crashes or hangs shortly after login
please try
230-using a dash (-) as the first character of your
password.  This will
230-turn off the informational messages that may be
confusing your FTP
230-client.
230-
230-Please send any comments to ftpadmin@earth.
230-
230 Guest login ok, access restrictions apply.
ftp> cd pub
250-Please read the file README
250-  it was last modified on Thu Jul 15 16:12:25 1999 - 0
days ago
250 CWD command successful.
ftp> get README /tmp/README
200 PORT command successful.
150 Opening ASCII mode data connection for README (0
bytes).
226 ASCII Transfer complete.
ftp> quit
221 Goodbye.
```

Steuern des Zugriffs auf Dateien auf dem FTP-Server

Die in diesem Abschnitt beschriebenen FTP-Server-Zugriffssteuerungsfunktionen ergänzen die standardmäßigen Datei- und Verzeichnis-Zugriffssteuerungsfunktionen, die in der Solaris-Version zur Verfügung stehen. Verwenden Sie die standardmäßigen Befehle, um festzulegen, welche Benutzer auf Dateien zugreifen, Dateien ändern oder Dateien hochladen können. Siehe dazu `chmod(1)`, `chown(1)` und `chgrp(1)`.

▼ So steuern Sie Dateizugriffsbefehle

Gehen Sie wie folgt vor, um mithilfe der Berechtigungsfunktionen in `ftpaccess` anzugeben, welche Benutzer welche Befehle ausführen können:

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie folgende Einträge in `ftpaccess` ein:**

command `yes|no` *typelist*

command	Die Befehle `ichmod`, `delete`, `overwrite`, `rename` oder `umask`
`yes|no`	Erlaubt oder verwehrt einem Benutzer das Ausgeben eines Befehls
typelist	Eine durch Komma getrennte Liste der Schlüsselwörter `anonymous`, `guest` und `real`

Beispiel 28–12 Steuern von Dateizugriffsbefehlen

Es folgen Beispiele für Berechtigungen, die für Dateizugriffsfunktionen auf dem FTP-Server definiert sind.

```
chmod no anonymous, guest
delete    no anonymous
overwrite no anonymous
rename    no anonymous
umask     no guest, anonymous
```

Im vorangegangenen Beispiel ist Folgendes definiert:

- Anonymen Benutzern ist nicht erlaubt, Dateien zu löschen, zu überschreiben oder umzubenennen.
- Gastbenutzern und anonymen Benutzern ist nicht erlaubt, Zugriffsmodi zu ändern und umask neu zu definieren.

Steuern von Uploads und Downloads auf dem FTP-Server

Sie können Uploads und Downloads auf dem FTP-Server steuern, indem Sie die Berechtigungen für die Verzeichnisse auf dem Server definieren. Standardmäßig sind anonymen Benutzern keine Uploads erlaubt. Lassen Sie Vorsicht walten, wenn Sie Uploads für anonyme Benutzer aktivieren.

▼ So steuern Sie Uploads auf den FTP-Server

Fügen Sie die Anweisungen in die `ftpaccess`-Datei ein, um Upload-Berechtigungen und Fehlermeldungen für fehlgeschlagene Uploads zu definieren.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:

Um Benutzern das Hochladen von Dateien zu ermöglichen, fügen Sie folgenden Eintrag ein:

```
upload [absolute|relative] [class=<classname>]... [-] root-dir \
dirglob yes|no owner group mode [dirs|nodirs] [<d_mode>]

path-filter typelist mesg allowed-charset {disallowed regexp...}
```

`upload`	Schlüsselwort, das für Benutzer verwendet wird, die ein Home-Verzeichnis (das Argument für `chroot()`) von *root-dir* haben. Das *root-dir*-Verzeichnis kann mit einem Sternchen (*) angegeben werden, wodurch Übereinstimmung mit allen Home-Verzeichnissen hergestellt wird.
`absolute|relative`	Parameter, der angibt, ob die *root-dir*-Verzeichnispfade als absolute oder relative Pfade zum aktuellen `chroot` -Verzeichnis interpretiert werden.
`class`	Schlüsselwort, das verwendet wird, um eine Reihe von `class=<classname>` -Beschränkungen zu definieren. Wenn Beschränkungen definiert sind, wird die Upload-Klausel nur dann wirksam, wenn der aktuelle Benutzer zu einer der angegebenen Klassen gehört.
root-dir	Das Root-Verzeichnis des Benutzers und das Home-Verzeichnis für anonyme Benutzer

dirglob	Eine Struktur zum Abgleichen eines Verzeichnisnamens. Ein Sternchen kann an jeder Stelle oder alleinstehend verwendet werden, um ein Verzeichnis darzustellen.
`yes|no`	Variable, die das Hochladen auf den FTP-Server erlaubt oder verwehrt
owner	Eigentümer von Dateien, die in `dirnames` hochgeladen werden
group	Gruppe, die Dateien zugeordnet ist, die in `dirnames` hochgeladen werden
mode	Parameter, der verwendet wird, um Zugriffsberechtigungen für hochgeladene Dateien anzugeben. Der standardmäßige Modus `0440` verhindert, dass hochgeladene Dateien über das anonyme Konto gelesen werden können.
`dirs|nodirs`	Schlüsselwort, das Benutzern erlaubt oder verwehrt, Unterverzeichnisse in einem Verzeichnis zu erstellen, das in `dirnames` aufgelistet ist
`d_mode`	Optionaler Modus zur Festlegung der Berechtigungen für ein neu erstelltes Verzeichnis
`path-filter`	Schlüsselwort zur Steuerung der Namen von hochgeladenen Dateien
typelist	Eine durch Komma getrennte Liste der Schlüsselwörter `anonymous`, `guest` und `real`
mesg	Eine angezeigte Meldungsdatei stimmt nicht mit den `regexp` -Kriterien überein
allowed-charset {disallowed regexp...}	Alphanumerische Zeichen, die in Dateinamen erlaubt oder nicht erlaubt sind

Beispiel 28–13 Steuern von Uploads auf den FTP-Server

```
upload /export/home/ftp /incoming yes ftpadm ftpadmin 0440 nodirs
path-filter anonymous /etc/ftpd/filename.msg ^[-A-Za-z0-9._]*$ ^[.-]
```

Im vorangegangenen Beispiel ist Folgendes definiert:

- FTP-Benutzerkonten, die `chroot` für `/export/home/ftp` verwenden, können Dateien in das `/incoming`-Verzeichnis hochladen. Hochgeladene Dateien sind im Besitz des Benutzers `ftpadm` und der Gruppe `ftpadmin`. Der Modus ist mit dem Schlüsselwort `nodirs` auf `0440` gesetzt, damit anonyme Benutzer keine Unterverzeichnisse erstellen können.
- Für anonyme Benutzer wird ein Dateiname durch eine Zeichenfolge von A–Z, a–z, 0–9 oder einen Punkt (.), Bindestrich (-) oder Unterstrich (_) dargestellt. Dateinamen können nicht mit einem Punkt (.) oder Bindestrich (-) beginnen. Wenn ein Dateiname diesen Filter nicht erfolgreich durchläuft, wird die `/etc/ftpd/filename.msg`-Meldung angezeigt, wenn der FTP-Administrator die Meldungsdatei erstellt hat. Dieser Meldung folgt eine FTP-Server-Fehlermeldung.

Die Eigentümerschaft und die Berechtigungen für ein Verzeichnis, in das Dateien anonym hochgeladen werden können, sollten einer strengen Kontrolle unterliegen. Der FTP-Administrator sollte der Eigentümer aller Dateien sein, die auf den FTP-Server hochgeladen werden. Sie müssen einen FTP-Administrator erstellen, wenn anonymen Benutzern erlaubt ist, Dateien hochzuladen. Das Verzeichnis muss im Besitz des Benutzers `ftpadm` und der Gruppe `ftpadm` sein, und die Berechtigungen müssen auf `3773` gesetzt sein.

Der Zugriffsmodus für Dateien, die auf den FTP-Server hochgeladen werden, muss `0440` sein. Der Modus `0440` verhindert, dass hochgeladene Dateien über das anonyme Konto gelesen werden können. Durch diese Beschränkung wird Ihr Server geschützt und kann nicht von Dritten für die Verteilung von Dateien verwendet werden.

Damit hochgeladene Dateien verteilt werden können, kann der FTP-Administrator die Dateien in ein öffentliches Verzeichnis verschieben.

▼ So steuern Sie Downloads auf den FTP-Server

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein, um zu verhindern, das Benutzer Dateien abrufen:

`noretrieve [absolute|relative] [class=`*classname*`]... [-]` *filename ...*

`noretrieve`	Schlüsselwort, mit dem verhindert wird, dass eine bestimmte Datei oder bestimmte Dateien abgerufen werden

`absolute|relative`	Parameter, der angibt, ob die *root-dir*-Verzeichnispfade als absolute oder relative Pfade zum aktuellen `chroot` -Verzeichnis interpretiert werden
`class`	Schlüsselwort, das verwendet wird, um `class=<classname>` für Benutzer zu definieren, für die `noretrieve`-Beschränkungen gelten
filename	Name der Datei, deren Abruf dem Benutzer nicht erlaubt ist

Beispiel 28–14 Steuern von Downloads auf den FTP-Server

```
noretrieve /etc/passwd
```

Im vorangegangenen Beispiel wird allen Benutzern das Abrufen der `/etc/passwd`-Datei verwehrt.

Virtuelles Hosting

Virtuelles Hosting erlaubt dem FTP-Server, mehrere Domains auf demselben Rechner zu unterstützen. Jeder virtuelle Host benötigt eine separate logische Schnittstelle und eine IP-Adresse.

Der FTP-Server unterstützt zwei Arten des virtuellen Hosting: *limitiert* und *komplett*. Beim limitierten virtuellen Hosting werden dieselben Konfigurationsdateien für alle virtuellen Hosts verwendet. Beim kompletten virtuellen Hosting können separate Konfigurationsdateien für jeden virtuellen Host verwendet werden.

Hinweis – Standardmäßig ist es authentischen und Gastbenutzern nicht erlaubt, sich bei virtuellen Hosts anzumelden. Sie können die folgenden `ftpaccess`-Anweisungen definieren, um die Standardeinstellung außer Kraft zu setzen.

```
To allow access to specific users:
virtual address allow username
To deny access to anonymous users:
virtual address private username
```

Weitere Informationen finden Sie unter `ftpaccess(4)`.

▼ So aktivieren Sie das limitierte virtuelle Hosting

Das limitierte virtuelle Hosting bietet teilweise Unterstützung für virtuelle FTP-Server. Sie können Unterstützung für das limitierte virtuelle Hosting aktivieren, indem Sie das virtuelle Root-Verzeichnis angeben. Sie können auch nach Bedarf die folgenden Parameter für den virtuellen Host in der `ftpaccess`-Datei angeben:

- `banner`
- `logfile`
- `email`
- `hostname`

Alle in der `ftpaccess`-Datei enthaltenen Anweisungen werden auf allen virtuellen Servern gemeinsam genutzt.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:

```
virtual address root|banner|logfile path
virtual address hostname|email string
```

`virtual`	Schlüsselwort, dass verwendet wird, um Funktionen von virtuellen Servern zu aktivieren
address	IP-Adresse des virtuellen Servers
`root`	Das Stammverzeichnis des virtuellen Servers
`banner`	Bannerdatei, die angezeigt wird, wenn eine Verbindung mit dem virtuellen Server hergestellt wird
`logfile`	Datensatz von Dateiübertragungen zum und vom virtuellen Server
path	Variable, die verwendet wird, um den Speicherort von Verzeichnissen und Dateien auf dem virtuellen Server anzugeben
`email`	E-Mail-Adresse, die in Meldungsdateien und im `HELP` -Befehl verwendet wird
`hostname`	Name des Hosts, der in der Begrüßungsmeldung oder im Statusbefehl angezeigt wird
string	Variable, die verwendet wird, um `email`- oder `hostname`-Parameter anzugeben

Hinweis – Es ist möglich, `hostname` als Adresse des virtuellen Servers zu verwenden. Allerdings wird nachdrücklich empfohlen, stattdessen die IPv4-Adresse zu verwenden. DNS muss verfügbar sein, wenn die FTP-Verbindung empfangen wird, damit `hostname` abgeglichen werden kann. Bei einem IPv6-Host verwenden Sie den Hostnamen anstelle der IPv6-Adresse.

Beispiel 28–15 Aktivieren des limitierten virtuellen Hosting in der `ftpaccess`-Datei

```
virtual 10.1.2.3 root    /var/ftp/virtual/ftp-serv
virtual 10.1.2.3 banner  /var/ftp/virtual/ftp-serv/banner.msg
virtual 10.1.2.3 logfile /var/log/ftp/virtual/ftp-serv/xferlog
```

Das vorangegangene Beispiel zeigt, wie der Speicherort des `root`-Verzeichnisses sowie `banner` und `logfile` auf einem virtuellen FTP-Server festgelegt werden.

Beispiel 28–16 Aktivieren des limitierten virtuellen Hosting über die Befehlszeile

Limitierte virtuelle Hosts können mithilfe des `ftpaddhost(1M)`-Skripts und der Option `-l` definiert werden.

Im folgenden Beispiel wird `ftpaddhost` mit den Optionen `-l -b -x` ausgeführt, um limitiertes virtuelles Hosting mit einem Testbanner und der Protokolldatei `/var/ftp/virtual/10.1.2.3/xferlog` unter einem virtuellen Root-Verzeichnis `/var/ftp/virtual/10.1.2.3` zu konfigurieren.

```
# ftpaddhost -l -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

▼ So aktivieren Sie komplettes virtuelles Hosting

Komplettes virtuelles Hosting erlaubt, separate Konfigurationsdateien für jede virtuelle Domain zu verwenden. Um komplettes virtuelles Hosting auf dem FTP-Server zu aktivieren, können Sie die folgenden FTP-Konfigurationsdateien für bestimmte Domains erstellen oder modifizieren:

- `ftpaccess`
- `ftpusers`
- `ftpgroups`
- `ftphosts`
- `ftpconversions`

Weitere Informationen finden Sie unter `ftpaccess(4)`, `ftpusers(4)`, `ftpgroups(4)`, `ftphosts(4)` und `ftpconversions(4)`.

Hinweis – Wenn keine separaten Versionen der Konfigurationsdateien zur Verfügung stehen, werden die Stammversionen der Dateien im `/etc/ftpd`-Verzeichnis verwendet.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Fügen Sie den folgenden Eintrag in die `/etc/ftpd/ftpservers` -Datei ein:**

   address /config-file-dir

address	IP-Adresse des virtuellen Servers
config-file-dir	Verzeichnis, das die Konfigurationsdateien enthält, die für den virtuellen Host angepasst werden

   Hinweis – Es ist möglich, `hostname` als Adresse des virtuellen Servers zu verwenden. Allerdings wird nachdrücklich empfohlen, stattdessen die IPv4-Adresse zu verwenden. DNS muss verfügbar sein, wenn die FTP-Verbindung empfangen wird, damit `hostname` abgeglichen werden kann. Bei einem IPv6-Host verwenden Sie den Hostnamen anstelle der IPv6-Adresse.

3. **Um eine angepasste Version einer FTP-Serverkonfigurationsdatei für den virtuellen Host zu erstellen, kopieren Sie die Stammversion der Datei aus dem `/etc/ftpd`-Verzeichnis in das `/config-file-dir`-Verzeichnis.**

   Weitere Informationen finden Sie unter `ftpservers(4)`.

Beispiel 28–17 Aktivieren des kompleten virtuellen Hosting in der `ftpservers`-Datei

```
#
# FTP Server virtual hosting configuration file
#

10.1.2.3 /net/inet/virtual/somedomain/
10.1.2.4 /net/inet/virtual/anotherdomain/
```

Im vorangegangenen Beispiel werden die IP-Adressen für zwei verschiedene Domains auf dem virtuellen Server angegeben.

Beispiel 28–18 Aktivieren des kompletten virtuellen Hosting über die Befehlszeile

Komplette virtuelle Hosts können mithilfe des `ftpaddhost(1M)`-Skripts und der Option `-c` definiert werden.

Im folgenden Beispiel wird `ftpaddhost` mit den Optionen `-c -b -x` ausgeführt, um komplettes virtuelles Hosting mit einem Testbanner und der Protokolldatei `/var/ftp/virtual/10.1.2.3/xferlog` unter einem virtuellen Root-Verzeichnis (`/var/ftp/virtual/10.1.2.3`) zu konfigurieren.

```
# ftpaddhost -c -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

Automatisches Starten des FTP-Servers

Es gibt drei Möglichkeiten, den FTP-Server zu starten:

- Als `nowait`-Server, der durch `inetd` gestartet wird
- Als eigenständigen Server, der im Hintergrund ausgeführt wird
- Als eigenständigen Server, der im Vordergrund und über die `inittab` -Datei ausgeführt wird

Ein eigenständiger Server antwortet immer am schnellsten und ist für große Server vorgesehen, die eigens zur Bereitstellung des FTP-Service dienen. Der eigenständige Server bietet eine geringe Verbindungslatenz für dedizierte Server, da das eigenständige System nie neu gestartet werden muss. Der eigenständige Server wird immer ausgeführt – sogar außerhalb der Hauptzeiten – und wartet unbegrenzt lange auf Verbindungen.

▼ So starten Sie einen FTP-Server mithilfe von SMF

Standardmäßig ist der SMF-Service konfiguriert, wodurch der FTP-Server mithilfe des `nowait`-Modus gestartet wird. Wenn der Standort viele Verbindungen verarbeitet, kann der FTP-Server auch im eigenständigen Modus ausgeführt werden. Informationen zu weiteren Befehlszeilenoptionen finden Sie auf der Manpage `in.ftpd(1M)`.

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Prüfen Sie die `wait`-Eigenschaft für den FTP-Server.

Die Zeile, mit der `wait=FALSE` gemeldet wird, zeigt an, dass der Server im `nowait`-Modus gestartet wird.

```
# inetadm -l network/ftp
SCOPE    NAME=VALUE
         name="ftp"
         endpoint_type="stream"
```

```
        proto="tcp6"
        isrpc=FALSE
        wait=FALSE
        exec="/usr/sbin/in.ftpd -a"
        user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=FALSE
```

3 Starten Sie den FTP-Server.

```
# svcadm enable network/ftp
```

▼ So starten Sie einen eigenständigen FTP-Server im Hintergrund

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 Deaktivieren Sie den FTP-Server.

```
# svcadm disable network/ftp
```

3 Starten Sie den eigenständigen FTP-Server.

```
# /usr/sbin/in.ftpd -a -S
```

Fügen Sie die Zeile in ein FTP-Server-Startskript ein. Informationen zum Erstellen eines Systemstartskripts finden Sie unter „Using Run Control Scripts“ in *System Administration Guide: Basic Administration*.

▼ So starten Sie einen eigenständigen FTP-Server im Vordergrund

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Deaktivieren Sie den FTP-Server.**

```
# svcadm disable network/ftp
```

3 **Fügen Sie einen Eintrag in die `inittab`-Datei ein, um den Service zu starten.**

Der neue Eintrag in `/etc/inittab` sollte folgendes Aussehen haben:

```
ftpd:3:respawn:/usr/sbin/in.ftpd -a -s
```

4 **Weisen Sie `init` an, `/etc/inittab` erneut zu prüfen.**

Mithilfe dieses Befehls wird der FTP-Service gestartet.

```
# init q
```

Abschalten des FTP-Servers

Mit dem Befehl `ftpshut(1M)` wird der FTP-Server zu einer bestimmten Zeit abgeschaltet.

Wenn Sie `ftpshut` ausführen, wird eine Datei generiert, die auf Befehlszeilenoptionen basiert, mit deren Hilfe festgelegt ist, wann Abschaltungen durchgeführt, neue Verbindungen abgelehnt und bestehende Verbindungen unterbrochen werden. Basierend auf diesen Informationen werden Benutzer von der Abschaltung des Servers in Kenntnis gesetzt. Der Speicherort der Datei, die durch `ftpshut` erstellt wird, ist durch die `shutdown`-Anweisung in der `ftpaccess`-Datei definiert.

▼ So schalten Sie den FTP-Server ab

Anhand des folgenden Verfahrens können Sie `ftpshut` ausführen und die `shutdown`-Anweisung in die `ftpaccess`-Datei einfügen.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2 **Fügen Sie folgende Einträge in die `ftpaccess` -Datei ein:**

`shutdown` *path*

`shutdown`	Schlüsselwort zur Angabe des Pfads zu einer Datei, die regelmäßig geprüft wird, um festzustellen, ob der FTP-Server planmäßig abgeschaltet werden soll
path	Speicherort der Datei, die durch den Befehl `ftpshut` erstellt wurde

3 **Führen Sie den Befehl `ftpshut` aus.**

```
ftpshut [ -V ] [ -l min] [ -d min] time [warning-message...]
```

`ftpshut`	Befehl zur Bereitstellung eines Verfahrens, das dazu dient, Benutzer über die Abschaltung des FTP-Servers zu benachrichtigen
`-V`	Option, die dazu dient, Urheberrechts- und Versionsinformationen anzuzeigen und den Vorgang anschließend zu beenden
`-l`	Flag, das verwendet wird, um einen Zeitpunkt zu definieren, an dem neue Verbindungen mit dem FTP-Server abgelehnt werden
`-d`	Flag, das verwendet wird, um einen Zeitpunkt zu definieren, an dem bestehende Verbindungen mit dem FTP-Server getrennt werden
`time`	Abschaltzeit, die mit dem Wort `now` definiert wird, um eine sofortige Abschaltung festzulegen, oder mit einem der beiden Formate (+ *Zahl* oder *HHMM*), um eine spätere Abschaltung festzulegen
`[warning-message...]`	Abschaltungsmeldung

4 **Verwenden Sie den Befehl `ftprestart`, um den FTP-Server nach einer Abschaltung neu zu starten.**

Weitere Informationen finden Sie auf den Manpages `ftpshut`(1M), `ftpaccess`(4) und `ftprestart`(1M).

Beheben von FTP-Serverproblemen

In diesem Abschnitt werden einige der Möglichkeiten beschrieben, wie Probleme mit dem FTP-Server behoben werden können.

▼ So prüfen Sie `syslogd` auf FTP-Servermeldungen

Der FTP-Server schreibt Meldungen, die hilfreich für die Fehlersuche am Standort sind, der für Dämonmeldungen in der `/etc/syslog.conf`-Datei definiert ist. Wenn ein Problem mit dem FTP-Server auftritt, stellen Sie zunächst fest, ob in dieser Datei derartige Meldungen vorhanden sind.

Die Meldungen des FTP-Servers werden vom Dämon der Einrichtung und durch Informationen gesteuert, die sich auf die Systemebene beziehen. Gehen Sie wie folgt vor, um Meldungen vom FTP-Server an `/var/adm/message` zu senden und von `syslogd` erneut die zugehörige Konfigurationsdatei lesen zu lassen:

1. **Fügen Sie einen Eintrag wie den folgenden in die `/etc/syslog.conf`-Datei ein:**

   ```
   daemon.info /var/adm/message
   ```

2. **Weisen Sie `syslogd` an, die zugehörige Konfiguration erneut zu lesen.**

   ```
   # svcadm refresh system/system-log
   ```

   Dieser Vorgang bewirkt, dass informative Meldungen des FTP-Servers in `/var/adm/messages` geschrieben werden.

▼ So verwenden Sie `greeting text`, um `ftpaccess` zu prüfen

Gehen Sie wie folgt vor, um mithilfe der `greeting text`-Funktion sicherzustellen, dass die richtige `ftpaccess`-Datei verwendet wird:

1. **Fügen Sie die folgende Anweisung in die ftpaccess-Datei ein.**

   ```
   greeting text message
   ```

2. **Stellen Sie eine Verbindung mit dem FTP-Server her.**

3. **Gehen Sie wie folgt vor, wenn die Meldung nicht angezeigt wird:**

   a. **Stellen Sie sicher, dass sich die `ftpaccess`-Datei am richtigen Speicherort befindet. Verwenden Sie den Befehl `strings(1)`, um den Speicherort der Datei aus der Binärdatei des FTP-Servers abzurufen.**

      ```
      # strings /usr/sbin/in.ftpd | grep "^/.*ftpaccess"
      ```

b. Prüfen Sie die `ftpservers`-Datei, um festzustellen, ob das virtuelle Hosting konfiguriert wurde.

Weitere Informationen finden Sie unter `ftpaccess(4)`, `ftpservers(4)`, `strings(1)`, `syslog.conf(4)` und `pgrep(1)`.

▼ So stellen Sie fest, welche Befehle von FTP-Benutzern ausgeführt wurden

Um festzustellen, welche Befehle von FTP-Benutzern ausgeführt werden, verwenden Sie die `log commands`-Protokollierfunktion in `ftpaccess`.

1 Fügen Sie die folgende Anweisung in die `ftpaccess` -Datei ein, um Befehle von Benutzern zu protokollieren, die in *typelist* angegeben sind.

```
log commands typelist
```

2 Prüfen Sie die Meldungen, die sich an dem Speicherort befinden, der in der `/etc/syslog.conf`-Datei angegeben ist.

Konfigurationshilfe für Standorte mit hoher Auslastung

Die folgende Liste enthält Empfehlungen zur Verbesserung der Leistung von FTP-Standorten.

1. Bei Standorten, die normalerweise mehrere gleichzeitige Verbindungen unterstützen, sollte der FTP-Server im eigenständigen Modus laufen (siehe „Automatisches Starten des FTP-Servers“ auf Seite 671).
2. Verwenden Sie `vmstat` und andere Systemdienstprogramme, um das Host-System des FTP-Servers zu überwachen. Wenn die Ressourcen des Systems knapp werden, beschränken Sie die Anzahl der gleichzeitigen Verbindungen (siehe „So beschränken Sie Benutzeranmeldungen“ auf Seite 650). Weitere Informationen zur Systemüberwachung finden Sie in Kapitel 13, „Monitoring System Performance (Tasks)“ in *System Administration Guide: Advanced Administration*.
3. Wenn Sie ein Verbindungslimit einrichten, sollten Sie die `limit-time` - und `timeout idle`-Funktionen in der `ftpaccess` -Datei verwenden. Dadurch wird unterbunden, dass Benutzer Verbindungen belegen. Wenn Sie kein Verbindungslimit einrichten, geben Sie die Option `-Q` für `in.ftpd` an.
4. Wenn Sie keine FTP-An- und -Abmeldungsdatensätze in `/var/adm/wtmpx` benötigen, geben Sie die Option `-W` für `in.ftpd` an.

5. Um die Belastung des Systems zu verringern, das den FTP-Server hostet, erhöhen Sie die Transferpuffergrößen, indem Sie die `recvbuf`- und `sendbuf` -Funktionen in der `ftpaccess`-Datei verwenden. Wenn große Puffergrößen gewählt werden, kann es nötig sein, mithilfe der `timeout data`-Funktion in der `ftpaccess` -Datei das Zeitlimit für Datentransfers zu erhöhen.
6. Der FTP-Server liest Daten aus verschiedenen Datenbanken, darunter Daten von Hosts, Passworteinträgen, Gruppen und Services. Langsame Suchvorgänge führen zu bedeutenden Verzögerungen der Anmeldung beim FTP-Server. Darum sollte zunächst die `files`-Quelle in der `nsswitch.conf`-Datei konfiguriert werden, um die Suchzeiten zu minimieren. Weitere Informationen finden Sie auf der Manpage `nsswitch.conf(4)`.
7. Der FTP-Server versucht standardmäßig, den Namen des Remote-Hosts zu finden. Dieser Vorgang kann langwierig sein und zu einer bedeutenden Verzögerung der Anmeldung führen. Dieser Suchvorgang kann mithilfe der `rhostlookup` -Funktion in der `ftpaccess`-Datei unterbunden werden. Beachten Sie jedoch Folgendes: Wenn keine Suche nach dem Namen des Remote-Hosts stattfindet, andere Funktionen in der `ftpaccess`-Datei verwendet werden und Übereinstimmung mit den Einträgen in der `ftphosts`-Datei besteht, wird nur die IP-Adresse des Remote-Hosts abgeglichen. Außerdem wird die IP-Adresse des Remote-Hosts in den Meldungen und anstelle des magischen Cookie (%R) verwendet. Eine Beschreibung der `rhostlookup`-Funktion finden Sie auf der Manpage `ftpaccess(4)`.
8. Auch kann das Abrufen von Kontingentinformationen die Anmeldung beim FTP-Server stark verzögern. Aus diesem Grunde sollten Sie die `quota-info`-Funktion in der `ftpaccess`-Datei nur dann verwenden, wenn Sie die magischen Kontingent-Cookies verwenden. Eine Liste der magischen Kontingent-Cookies finden Sie auf der Manpage `ftpaccess(4)`.

◆ ◆ ◆ KAPITEL 29

Zugriff auf Remote-Systeme (Aufgaben)

In diesem Kapitel werden sämtliche Aufgaben beschrieben, die für die Anmeldung bei Remote-Systemen und das Arbeiten mit den Dateien dieser Systeme erforderlich sind. Es folgt eine Liste von schrittweisen Anweisungen:

- „Zugriff auf Remote-Systeme (Übersicht der Schritte)“ auf Seite 679
- „Anmelden bei einem Remote-System (`rlogin`)“ auf Seite 680
- „Anmelden bei einem Remote-System (`ftp`)“ auf Seite 688
- „Remote-Kopieren mit `rcp`“ auf Seite 695

Zugriff auf Remote-Systeme (Übersicht der Schritte)

Die in diesem Kapitel enthaltenen Aufgaben, die in der folgenden Tabelle beschrieben werden, dienen zum Anmelden bei und zum Kopieren von Dateien aus Remote-Systemen.

TABELLE 29–1 Übersicht der Schritte: Zugriff auf Remote-Systeme

Aufgabe	Beschreibung	Siehe
Anmelden bei einem Remote-System (`rlogin`)	■ Entfernen Sie die `.rhosts`-Dateien. ■ Führen Sie den Befehl `rlogin` aus, um auf ein Remote-System zuzugreifen.	„So gehen Sie vor, um nach `.rhosts`-Dateien zu suchen und diese zu entfernen“ auf Seite 685 „So stellen Sie fest, ob ein Remote-System funktioniert“ auf Seite 686 „So stellen Sie fest, wer bei einem Remote-System angemeldet ist“ auf Seite 686 „So melden Sie sich bei einem Remote-System an (`rlogin`)“ auf Seite 687 „So melden Sie sich bei einem Remote-System ab (`exit`)“ auf Seite 688

TABELLE 29–1 Übersicht der Schritte: Zugriff auf Remote-Systeme *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
Anmelden bei einem Remote-System (ftp)	■ Öffnen und schließen Sie eine ftp-Verbindung. ■ Kopieren Sie Dateien auf und von einem Remote-System.	„So öffnen Sie eine ftp-Verbindung mit einem Remote-System“ auf Seite 690 „So schließen Sie eine ftp-Verbindung mit einem Remote-System“ auf Seite 691 „So kopieren Sie Dateien aus einem Remote-System (ftp)“ auf Seite 691 „So kopieren Sie Dateien in ein Remote-System (ftp)“ auf Seite 693
Kopieren von Remote-Dateien mit rcp	Führen Sie den Befehl rcp aus, um Dateien auf ein Remote-System und von einem Remote-System zu kopieren.	„So kopieren Sie Dateien zwischen einem lokalen System und einem Remote-System (rcp)“ auf Seite 698

Anmelden bei einem Remote-System (rlogin)

Mit dem Befehl rlogin können Sie sich bei einem Remote-System anmelden. Sobald Sie angemeldet sind, können Sie im Remote-Dateisystem navigieren und die in ihm enthaltenen Inhalte (in Abhängigkeit von Ihren Berechtigungen) bearbeiten, Dateien kopieren oder Remote-Befehle ausführen.

Wenn sich das System, bei dem Sie sich anmelden, in einer Remote-Domain befindet, muss der Domainname unbedingt an den Systemnamen angefügt werden. In diesem Beispiel ist SOLAR der Name der Remote-Domain:

```
rlogin pluto.SOLAR
```

Sie können eine Remote-Anmeldung jederzeit unterbrechen, indem Sie Strg-d drücken.

Authentifizierung für Remote-Anmeldungen (rlogin)

Die Authentifizierung (d. h. die Prüfung Ihrer Identität) für rlogin-Vorgänge kann entweder vom Remote-System oder vom Netzwerk durchgeführt werden.

Der Hauptunterschied zwischen diesen Formen der Authentifizierung liegt in der Interaktion, die von Ihnen verlangt wird, und in der Art und Weise, wie die jeweilige Authentifizierung durchgeführt wird. Wenn ein Remote-System versucht, Sie zu authentifizieren, werden Sie zur Eingabe eines Passworts aufgefordert, es sei denn, Sie richten die Datei /etc/hosts.equiv oder die Datei .rhosts entsprechend ein. Wenn das Netzwerk versucht, Sie zu authentifizieren, werden Sie nicht zur Eingabe eines Passworts aufgefordert, da Ihre Identität dem Netzwerk bereits bekannt ist.

Wenn ein Remote-System versucht, Sie zu authentifizieren, verlässt es sich auf die Informationen in seinen lokalen Dateien. Dies trifft insbesondere unter folgenden Bedingungen zu:

- Ihr Systemname und Ihr Benutzername sind in der `/etc/hosts.equiv`-Datei des Remote-Systems angegeben.
- Ihr Systemname und Ihr Benutzername sind in der `.rhosts` -Datei des Remote-Benutzers angegeben, die sich im Home-Verzeichnis des Remote-Benutzers befindet.

Zur Netzwerkauthentifizierung werden eine der beiden folgenden Methoden verwendet:

- Eine vertrauenswürdige Netzwerkumgebung wird mithilfe Ihres lokalen Netzwerkinformationsservice und des Automounters eingerichtet.
- Die `/etc/nsswitch.conf`-Datei verweist auf einen der Netzwerkinformationsservices, der Informationen über Sie bereithält.

Hinweis – Die Systemauthentifizierung wird im Allgemeinen durch die Netzwerkauthentifizierung ersetzt.

`/etc/hosts.equiv`-Datei

Die `/etc/hosts.equiv`-Datei enthält eine Liste von vertrauenswürdigen Hosts für ein Remote-System (jeweils einer pro Zeile). Wenn ein Benutzer versucht, sich (mithilfe von `rlogin`) über einen der in dieser Datei aufgeführten Hosts anzumelden, und wenn das Remote-System auf den Passworteintrag des Benutzers zugreifen kann, lässt das System zu, dass der Benutzer sich ohne Passwort anmeldet.

Eine typische `hosts.equiv`-Datei ist wie folgt aufgebaut:

```
host1
host2 user_a
+@group1
-@group2
```

Wenn ein einfacher Eintrag für einen Host in `hosts.equiv` erfolgt (beispielsweise ein Eintrag wie `host1` im obigen Beispiel), bedeutet das, dass der Host als vertrauenswürdig betrachtet wird. Dies gilt dann auch für jeden Benutzer des Rechners.

Wenn auch der Benutzername (wie im zweiten Eintrag des Beispiels) angegeben wird, wird der Host nur dann als vertrauenswürdig betrachtet, wenn der angegebene Benutzer versucht, Zugang zu erhalten.

Wenn vor einem Gruppennamen ein Pluszeichen (+) steht, werden alle Rechner in der Netzgruppe als vertrauenswürdig betrachtet.

Wenn vor einem Gruppennamen ein Minuszeichen (–) steht, wird keiner der Rechner in dieser Netzgruppe als vertrauenswürdig betrachtet.

Sicherheitsrisiken beim Verwenden der /etc/hosts.equiv -Datei

Die /etc/hosts.equiv-Datei ist ein Sicherheitsrisiko. Wenn auf Ihrem System eine /etc/hosts.equiv-Datei vorhanden ist, sollten Sie nur vertrauenswürdige Hosts in Ihr Netzwerk aufnehmen. In der Datei sollten weder Hosts enthalten sein, die zu einem anderen Netzwerk gehören, noch Rechner, die in öffentlichen Bereichen eingesetzt werden. Sie sollten beispielsweise keinen Host aufnehmen, der sich in einer Zentrale befindet.

Wenn keine vertrauenswürdigen Hosts verwendet werden, können schwerwiegende Sicherheitsprobleme auftreten. Entweder ersetzen Sie die /etc/hosts.equiv-Datei durch eine richtig konfigurierte Datei, oder Sie entfernen die Datei gänzlich.

Eine einzelne Zeile mit Pluszeichen (+) in der /etc/hosts.equiv -Datei bedeutet, dass jeder bekannte Host als vertrauenswürdig betrachtet wird.

.rhosts-Datei

Die .rhosts-Datei ist das Benutzeräquivalent der /etc/hosts.equiv-Datei. Diese Datei enthält in der Regel eine Liste von Kombinationen aus Hosts und Benutzern anstelle von Hosts. Wenn eine Host-Benutzer-Kombination in dieser Datei aufgeführt ist, erhält der angegebene Benutzer die Berechtigung, sich ohne Passwort über den angegebenen Host anzumelden.

Beachten Sie, dass eine .rhosts-Datei sich auf der obersten Ebene des Home-Verzeichnisses eines Benutzers befinden muss. .rhost-Dateien, die sich in Unterverzeichnissen befinden, werden nicht abgefragt.

Benutzer können .rhosts-Dateien in ihren Home-Verzeichnissen erstellen. Die Verwendung der .rhosts-Datei ist eine weitere Möglichkeit, für vertrauenswürdigen Zugriff zwischen den Konten der Benutzer auf verschiedenen Systemen zu sorgen, ohne dass die /etc/hosts.equiv-Datei verwendet wird.

Sicherheitsrisiken beim Verwenden der .rhosts -Datei

Leider stellt die .rhosts-Datei ein großes Sicherheitsproblem dar. Während die /etc/hosts.equiv-Datei vom Systemadministrator kontrolliert wird und effizient verwaltet werden kann, kann jeder Benutzer die .rhosts-Datei erstellen und mithilfe dieser Datei jedem anderen Benutzer Zugriff gewähren, ohne dass der Systemadministrator davon Kenntnis hat.

Wenn sich alle Home-Verzeichnisse der Benutzer auf einem einzelnen Server befinden und nur bestimmte Personen Superuser-Zugriff auf diesen Server haben, können Sie die Verwendung einer .rhosts-Datei verhindern, indem Sie sich als Superuser anmelden und eine leere Datei in den Home-Verzeichnissen der Benutzer erstellen. Dann setzen Sie die Berechtigungen in dieser Datei auf 000, wodurch es schwierig ist, sie zu ändern. Selbst für einen Superuser wäre dies kein leichtes Unterfangen. Durch diese Änderung wird ein Benutzer daran gehindert, die Systemsicherheit durch unverantwortliche Verwendung einer .rhosts-Datei zu gefährden. Die Änderung hat jedoch keine Auswirkungen, wenn der Benutzer in der Lage ist, den Pfad zu seinem Home-Verzeichnis zu ändern.

Die einzige Möglichkeit, eine Gefährdung der Sicherheit auszuschließen, besteht darin, den Zugriff auf .rhosts-Dateien komplett zu unterbinden. Ausführliche Informationen zur Vorgehensweise finden Sie unter „So gehen Sie vor, um nach .rhosts-Dateien zu suchen und diese zu entfernen“ auf Seite 685. Als Systemadministrator können Sie das System häufig auf Verletzungen dieser Sicherheitsrichtlinie überprüfen. Ein mögliche Ausnahme zu dieser Richtlinie betrifft das Root-Konto. Eventuell benötigen Sie eine .rhosts-Datei, um Netzwerksicherungen und andere Remote-Services auszuführen.

Sequenzielle Remote-Anmeldungen

Wenn Ihr System richtig konfiguriert ist, können Sie sequentielle Remote-Anmeldungen durchführen. Beispiel: Ein Benutzer auf earth meldet sich bei jupiter an und beschließt, sich von dort bei pluto anzumelden.

Der Benutzer könnte sich auch bei jupiter abmelden und sich dann direkt bei pluto anmelden, aber die erstere Art der Anmeldung ist bequemer.

Um sequentielle Remote-Anmeldungen ohne Angabe eines Passworts durchzuführen, muss die /etc/hosts.equiv-Datei oder die .rhosts-Datei richtig eingerichtet sein.

Direkte oder indirekte Remote-Anmeldungen

Mit dem Befehl rlogin können Sie sich direkt oder indirekt bei einem Remote-System anmelden.

Eine direkte Remote-Anmeldung wird mit dem standardmäßigen Benutzernamen durchgeführt, also mit dem Benutzernamen der Person, die gerade beim lokalen System angemeldet ist. Dies ist die gebräuchlichste Form der Remote-Anmeldung.

Ein indirekte Remote-Anmeldung wird mit einem anderen Benutzernamen durchgeführt, der während der Remote-Anmeldung bereitgestellt wird. Mit dieser Art der Remote-Anmeldung können Sie versuchen, sich von einer Workstation aus anzumelden, die Sie vorübergehend geliehen haben. Wenn Sie beispielsweise im Büro eines Mitarbeiters Dateien in Ihrem Home-Verzeichnis prüfen müssen, können Sie sich über das System des Mitarbeiters bei Ihrem System anmelden. Allerdings müssen Sie zu diesem Zweck eine indirekte Remote-Anmeldung durchführen und Ihren eigenen Benutzernamen angeben.

Die Abhängigkeiten zwischen direkten und indirekten Anmeldungen und der Authentifizierung sind in der folgenden Tabelle zusammengefasst.

TABELLE 29–2 Abhängigkeiten zwischen Anmeldung und Authentifizierung (rlogin)

Art der Anmeldung	Bereitstellung des Benutzernames durch	Authentifizierung	Passwort
direkt	System	Netzwerk	nicht erforderlich
		System	erforderlich
indirekt	Benutzer	Netzwerk	nicht erforderlich
		System	erforderlich

Vorgang nach der Remote-Anmeldung

Wenn Sie sich bei einem Remote-System anmelden, wird mithilfe des Befehls `rlogin` nach Ihrem Home-Verzeichnis gesucht. Wenn Ihr Home-Verzeichnis nicht mithilfe des Befehls `rlogin` gefunden werden kann, werden Sie dem Root-Verzeichnis (`/`) des Remote-Systems zugewiesen. Beispiel:

```
Unable to find home directory, logging in with /
```

Wenn Ihr Home-Verzeichnis jedoch mithilfe des Befehls `rlogin` gefunden werden kann, werden sowohl Ihre `.cshrc`-Datei als auch Ihre `.login`-Datei als Quelle verwendet. Darum ist Ihre Eingabeaufforderung nach einer Remote-Anmeldung Ihre standardmäßige Anmeldeaufforderung, und das aktuelle Verzeichnis ist dasselbe wie bei einer lokalen Anmeldung.

Wenn beispielsweise bei Ihrer normalen Eingabeaufforderung Ihr Systemname und Ihr Arbeitsverzeichnis angezeigt werden und Sie sich anmelden, ist Ihr Arbeitsverzeichnis Ihr Home-Verzeichnis, und Ihre Anmeldeaufforderung sieht wie folgt aus:

```
earth(/home/smith):
```

Wenn Sie sich dann bei einem Remote-System anmelden, wird eine ähnliche Anmeldeaufforderung angezeigt, und Ihr Arbeitsverzeichnis ist Ihr Home-Verzeichnis, unabhängig von dem Verzeichnis, in dem Sie den Befehl `rlogin` eingegeben haben:

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/smith):
```

Der einzige Unterschied besteht darin, dass der Name des Remote-Systems am Anfang der Eingabeaufforderung an die Stelle Ihres lokalen Systems tritt. Das Remote-Dateisystem liegt parallel zu Ihrem Home-Verzeichnis.

Wenn Sie das Verzeichnis in `/home` ändern und `ls` ausführen, wird Folgendes angezeigt:

```
earth(home/smith): cd ..
earth(/home): ls
smith  jones
```

So gehen Sie vor, um nach .rhosts-Dateien zu suchen und diese zu entfernen

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ in *Systemverwaltungshandbuch: Sicherheitsservices*.

2. **Suchen Sie nach .rhosts -Dateien und entfernen Sie diese, indem Sie den Befehl find(1) verwenden.**

   ```
   # find home-directories -name .rhosts -print -exec rm {} \;
   ```

home-directories	Identifiziert den Pfad zu dem Verzeichnis, in dem sich die Home-Verzeichnisse von Benutzern befinden. Beachten Sie, dass Sie mehrere Pfade eingeben können, um gleichzeitig nach mehreren Home-Verzeichnissen zu suchen.
`-name .rhosts`	Identifiziert den Dateinamen.
`-print`	Gibt den aktuellen Pfadnamen aus.
`-exec rm {} \;`	Teilt dem Befehl `find` mit, den Befehl `rm` auf alle Dateien anzuwenden, die mithilfe des entsprechenden Dateinamens identifiziert werden.

   Der Befehl `find` beginnt mit dem benannten Verzeichnis und sucht nach einer Datei namens `.rhosts`. Wird eine solche Datei gefunden, gibt `find` den Pfad auf dem Bildschirm aus und entfernt diese.

Beispiel 29–1 Suchen nach .rhosts-Dateien und Entfernen dieser Dateien

Im folgenden Beispiel wird nach `.rhosts`-Dateien in allen Home-Verzeichnissen des Benutzers gesucht, die sich im `/export/home` -Verzeichnis befinden. Dann werden diese Dateien entfernt.

```
# find /export/home -name .rhosts -print | xargs -i -t rm {} \;
```

So stellen Sie fest, ob ein Remote-System funktioniert

Stellen Sie fest, ob ein Remote-System funktioniert, indem Sie den Befehl ping ausführen.

```
$ ping system-name | ip-address
```

system-name Der Name des Remote-Systems

ip-address Die IP-Adresse des Remote-Systems

Der Befehl ping gibt eine der drei folgenden Meldungen zurück:

Statusmeldung	Erklärung
system-name is alive	Auf das System kann über das Netzwerk zugegriffen werden.
ping: unknown host *system-name*	Der Systemname ist unbekannt.
ping: no answer from *system-name*	Das System ist bekannt, aber es ist gerade nicht in Betrieb.

Wenn sich das System, das Sie mit "ping" ansteuern, in einer anderen Domain befindet, kann die zurückgegebene Meldung auch Routing-Informationen enthalten, die Sie ignorieren können.

Der Befehl ping hat einen Zeitüberschreitungswert von 20 Sekunden. Wenn nach Ablauf von 20 Sekunden keine Antwort empfangen wird, wird die dritte Meldung zurückgegeben. Sie können ping zwingen länger (oder kürzere Zeit) zu warten, indem Sie einen *Zeitüberschreitungswert* in Sekunden eingeben:

```
$ ping system-name | ip-address time-out
```

Weitere Informationen finden Sie auf der Manpage ping(1M).

So stellen Sie fest, wer bei einem Remote-System angemeldet ist

Stellen Sie fest, wer bei einem Remote-System angemeldet ist, indem Sie den Befehl rusers(1) ausführen.

```
$ rusers [-l] remote-system-name
```

rusers (Keine Optionen) Zeigt den Namen des Systems an, dem der Name des Benutzers folgt, der gerade angemeldet ist, einschließlich Root.

`-l` Zeigt zusätzliche Informationen über jeden Benutzer an: das Anmeldefenster des Benutzers, das Datum und die Uhrzeit der Anmeldung, die Dauer der Anmeldung und den Namen des Remote-Systems, über das sich der Benutzer angemeldet hat.

BEISPIEL 29–2 Feststellen, wer bei einem Remote-System angemeldet ist

Im folgenden Beispiel wird die Kurzausgabe von `rusers` dargestellt.

```
$ rusers pluto
pluto    smith  jones
```

Im folgenden Beispiel ist die lange Version von `rusers` zu sehen. Es wird angezeigt, dass zwei Benutzer beim Remote-System `starbug` angemeldet sind. Der erste Benutzer, der sich am 10. September über die Systemkonsole angemeldet hat, ist seit 137 Stunden und 15 Minuten angemeldet. Der zweite Benutzer hat sich am 14. September über ein Remote-System, `mars`, angemeldet.

```
$rusers -l starbug
root         starbug:console           Sep 10 16:13  137:15
rimmer       starbug:pts/0             Sep 14 14:37         (mars)
```

So melden Sie sich bei einem Remote-System an (`rlogin`)

Melden Sie sich bei einem Remote-System an, indem Sie den Befehl `rlogin(1)` verwenden.

```
$ rlogin [-l user-name] system-name
```

`rlogin` (Keine Optionen) Meldet Sie *direkt* beim Remote-System an, wobei Ihr aktueller Benutzername verwendet wird.

`-l` *user-name* Meldet Sie *indirekt* beim Remote-System an, wobei der von Ihnen angegebene Benutzername verwendet wird.

Wenn das Netzwerk versucht, Sie zu authentifizieren, werden Sie nicht zur Eingabe eines Passworts aufgefordert. Wenn das Remote-System versucht, Sie zu authentifizieren, werden Sie zur Eingabe eines Passworts aufgefordert.

Wenn der Vorgang erfolgreich durchgeführt wird, wird mithilfe des Befehls `rlogin` eine kurze Information über Ihre letzte Remote-Anmeldung bei diesem System, die Version des auf Ihrem Remote-System ausgeführten Betriebssystems und das Vorhandensein von Mails in Ihrem Home-Verzeichnis angezeigt.

BEISPIEL 29–3 Anmelden bei einem Remote-System (rlogin)

Das folgende Beispiel zeigt die Ausgabe einer direkten Remote-Anmeldung bei pluto. Der Benutzer wurde durch das Netzwerk authentifiziert.

```
$ rlogin starbug
Last login: Mon Jul 12 09:28:39 from venus
Sun Microsystems Inc.   SunOS 5.8       February 2000
starbug:
```

Das folgende Beispiel zeigt die Ausgabe einer indirekten Remote-Anmeldung bei pluto, wobei der Benutzer durch das Remote-System authentifiziert wird.

```
$ rlogin -l smith pluto
password: user-password
Last login: Mon Jul 12 11:51:58 from venus
Sun Microsystems Inc.   SunOS 5.8       February 2000
starbug:
```

So melden Sie sich bei einem Remote-System ab (exit)

Melden Sie sich bei einem Remote-System ab, indem Sie den Befehl exit(1) ausführen.

```
$ exit
```

BEISPIEL 29–4 Abmelden bei einem Remote-System (exit)

Das folgende Beispiel zeigt die Abmeldung des Benutzers smith beim System pluto:

```
$ exit
pluto% logout
Connection closed.
earth%
```

Anmelden bei einem Remote-System (ftp)

Der Befehl ftp öffnet die Benutzerschnittstelle zum FTP (File Transfer Protocol). Diese Benutzerschnittstelle, die als Befehlsinterpreter bezeichnet wird, ermöglicht Ihnen, sich bei einem Remote-System anzumelden und diverse Vorgänge mithilfe des Dateisystems auszuführen. Die wichtigsten Vorgänge sind in der nachstehenden Tabelle zusammengefasst.

Der Hauptvorteil von ftp gegenüber rlogin und rcp ist, dass für ftp nicht die Ausführung von UNIX auf dem Remote-System erforderlich ist. Das Remote-System muss jedoch für die TCP/IP-Kommunikation konfiguriert sein. rlogin bietet jedoch eine größere Auswahl von Dateimanipulationsbefehlen als ftp.

Authentifizierung für Remote-Anmeldungen (ftp)

Die Authentifizierung für ftp-Remote-Anmeldungen kann mithilfe von einer der beiden folgenden Methoden eingerichtet werden:

- Einbeziehen Ihres Passworteintrags in die /etc/passwd -Datei des Remote-Systems oder in eine äquivalente Map oder Tabelle für Netzwerkinformationen
- Einrichten eines anonymen ftp-Kontos auf dem Remote-System

Wichtige ftp-Befehle

TABELLE 29–3 Wichtige ftp-Befehle

Befehl	Beschreibung
ftp	Greift auf den ftp-Befehlsinterpreter zu.
ftp *remote-system*	Stellt eine ftp-Verbindung mit einem Remote-System her. Anweisungen finden Sie unter „So öffnen Sie eine ftp-Verbindung mit einem Remote-System“ auf Seite 690.
open	Führt eine Anmeldung beim Remote-System über den Befehlsinterpreter durch.
close	Führt eine Abmeldung beim Remote-System durch und kehrt zum Befehlsinterpreter zurück.
bye	Beendet den ftp-Befehlsinterpreter.
help	Listet alle ftp-Befehle auf oder gibt eine kurze Beschreibung der Funktionsweise des Befehls aus, wenn ein Name eines Befehls angegeben wird.
reset	Synchronisiert die Befehl-Antwort-Sequenz mit dem ftp-Remote-Server neu.
ls	Listet den Inhalt des Remote-Arbeitsverzeichnisses auf.
pwd	Zeigt den Namen des Remote-Arbeitsverzeichnisses an.
cd	Ändert das Remote-Arbeitsverzeichnis.

TABELLE 29–3 Wichtige ftp-Befehle *(Fortsetzung)*

Befehl	Beschreibung
`lcd`	Ändert das lokale Arbeitsverzeichnis.
`mkdir`	Erstellt ein Verzeichnis auf dem Remote-System.
`rmdir`	Löscht ein Verzeichnis auf dem Remote-System.
`get, mget`	Kopiert eine Datei (oder mehrere Dateien) aus dem Remote-Arbeitsverzeichnis in das lokale Arbeitsverzeichnis.
`put, mput`	Kopiert eine Datei (oder mehrere Dateien) aus dem lokalen Arbeitsverzeichnis in das Remote-Arbeitsverzeichnis.
`delete, mdelete`	Löscht eine Datei (oder mehrere Dateien) aus dem Remote-Arbeitsverzeichnis.

Weitere Informationen finden Sie unter `ftp(1)`.

▼ So öffnen Sie eine `ftp`-Verbindung mit einem Remote-System

1 Stellen Sie sicher, dass Sie für die Nutzung von `ftp` authentifiziert sind.

Sie benötigen die `ftp`-Authentifizierung (siehe „Authentifizierung für Remote-Anmeldungen (`ftp`)“ auf Seite 689).

2 Öffnen Sie eine Remote-System-Verbindung, indem Sie den `ftp`-Befehl verwenden.

```
$ ftp remote-system
```

Sobald die Verbindung hergestellt ist, werden eine Bestätigungsmeldung und eine Eingabeaufforderung angezeigt.

3 Geben Sie Ihren Benutzernamen ein.

```
Name (remote-system:user-name): user-name
```

4 Wenn Sie zur Eingabe Ihres Passworts aufgefordert werden, geben Sie Ihr Passwort ein.

```
331 Password required for user-name:
Password: password
```

Wenn das System, auf das Sie zugreifen, ein anonymes `ftp`-Konto hat, werden Sie aufgefordert, eine E-Mail-Adresse für das Passwort einzugeben. Wenn Ihr Passwort von der `ftp`-Schnittstelle akzeptiert wird, werden eine Bestätigungsmeldung und die (`ftp>`)-Eingabeaufforderung angezeigt.

Jetzt können Sie alle Befehle verwenden, die von der `ftp`-Schnittstelle bereitgestellt werden, einschließlich der Hilfe. Die wichtigsten Befehle sind in Tabelle 29–3 zusammengefasst.

Beispiel 29–5 Öffnen einer ftp-Verbindung mit einem Remote-System

Diese ftp-Sitzung wurde vom Benutzer smith auf dem Remote-System pluto eingerichtet:

```
$ ftp pluto
Connected to pluto.
220 pluto FTP server ready.
Name (pluto:smith): smith
331 Password required for smith:
Password: password
230 User smith logged in.
ftp>
```

So schließen Sie eine ftp-Verbindung mit einem Remote-System

Schließen Sie eine ftp-Verbindung mit einem Remote-System, indem Sie den Befehl bye ausführen.

```
ftp> bye
221-You have  transferred 0 bytes in 0 files.
221-Total traffic for this sessions was 172 bytes in 0 transfers.
221-Thanks you for using the FTP service on spdev.
221 Goodbye.
```

Eine Abschiedsmeldung wird angezeigt. Danach folgt Ihre normale Shell-Eingabeaufforderung.

▼ So kopieren Sie Dateien aus einem Remote-System (ftp)

1. **Wechseln Sie in ein Verzeichnis auf dem lokalen System, in das die Dateien aus dem Remote-System kopiert werden sollen.**

   $ **cd** *target-directory*

2. **Stellen Sie eine ftp-Verbindung her.**

   Informationen zur Vorgehensweise finden Sie unter „So öffnen Sie eine ftp-Verbindung mit einem Remote-System“ auf Seite 690.

3. **Wechseln Sie in das Quellverzeichnis.**

   ftp> **cd** *source-directory*

   Wenn Ihr System den Automounter verwendet, wird das Home-Verzeichnis des Remote-Systembenutzers parallel zu Ihrem Verzeichnis unter /home angezeigt.

4. **Stellen Sie sicher, dass Sie über eine Leseberechtigung für die Quelldateien verfügen.**

   ```
   ftp> ls -l
   ```

5. **Setzen Sie den Transfertyp auf `binary` .**

   ```
   ftp> binary
   ```

6. **Um eine einzelne Datei zu kopieren, verwenden Sie den Befehl `get`.**

   ```
   ftp> get filename
   ```

7. **Um mehrere Dateien zu kopieren, verwenden Sie den Befehl `mget`.**

   ```
   ftp> mget filename [filename ...]
   ```

   Sie können eine Reihe von individuellen Dateinamen bereitstellen und Platzhalterzeichen verwenden. Mithilfe des Befehls `mget` wird jede Datei einzeln kopiert, und Sie werden jedesmal zur Bestätigung aufgefordert.

8. **Schließen Sie die `ftp`-Verbindungen.**

   ```
   ftp> bye
   ```

Beispiel 29–6 Kopieren von Dateien aus einem Remote-System (`ftp`)

In diesem Beispiel öffnet der Benutzer `kryten` eine `ftp`-Verbindung mit dem System `pluto` und verwendet den Befehl `get`, um eine einzelne Datei aus dem `/tmp`-Verzeichnis zu kopieren.

```
$ cd $HOME
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34344)
(0 bytes).
filea
files
ps_data
226 ASCII Transfer complete.
53 bytes received in 0.022 seconds (2.39 Kbytes/s)
ftp> get filea
200 PORT command successful.
150 ASCII data connection for filea (129.152.221.238,34331)
(0 bytes).
221 Goodbye.
```

In diesem Beispiel verwendet derselbe Benutzer (kryten) den Befehl mget, um mehrere Dateien aus dem /tmp -Verzeichnis in sein Home-Verzeichnis zu kopieren. Beachten Sie, dass der Benutzer kryten die Möglichkeit hat, einzelne Dateien zu akzeptieren oder abzulehnen.

```
$ ftp> cd /tmp
250 CWD command successful.
ftp> ls files
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34345)
(0 bytes).
fileb
filec
filed
remote: files
21 bytes received in 0.015 seconds (1.36 Kbytes/s)
ftp> cd files
250 CWD command successful.
ftp> mget file*
mget fileb? y
200 PORT command successful.
150 ASCII data connection for fileb (129.152.221.238,34347)
(0 bytes).
226 ASCII Transfer complete.
mget filec? y
200 PORT command successful.
150 ASCII data connection for filec (129.152.221.238,34348)
(0 bytes).
226 ASCII Transfer complete.
mget filed? y
200 PORT command successful.
150 ASCII data connection for filed (129.152.221.238,34351)
(0 bytes).
226 ASCII Transfer complete.200 PORT command successful.
ftp> bye
221 Goodbye.
```

▼ So kopieren Sie Dateien in ein Remote-System (ftp)

1 Wechseln Sie in das Quellverzeichnis auf dem lokalen System.

Das Verzeichnis, in dem Sie den ftp-Befehl eingeben, ist das lokale Arbeitsverzeichnis und somit auch das Quellverzeichnis für diesen Vorgang.

2 Stellen Sie eine ftp-Verbindung her.

Informationen zur Vorgehensweise finden Sie unter „So öffnen Sie eine ftp-Verbindung mit einem Remote-System“ auf Seite 690.

3 Wechseln Sie in das Zielverzeichnis.

ftp> **cd** *target-directory*

Wenn Ihr System den Automounter verwendet, wird das Home-Verzeichnis des Remote-Systembenutzers parallel zu Ihrem Verzeichnis unter /home angezeigt.

4 Stellen Sie sicher, dass Sie über eine Schreibberechtigung für das Zielverzeichnis verfügen.

```
ftp> ls -l target-directory
```

5 Setzen Sie den Transfertyp auf "binary".

```
ftp> binary
```

6 Um eine einzelne Datei zu kopieren, verwenden Sie den Befehl put.

```
ftp> put filename
```

7 Um mehrere Dateien zu kopieren, verwenden Sie den Befehl mput.

```
ftp> mput filename [filename ...]
```

Sie können eine Reihe von individuellen Dateinamen bereitstellen und Platzhalterzeichen verwenden. Mithilfe des Befehls mput wird jede Datei einzeln kopiert, und Sie werden jedesmal zur Bestätigung aufgefordert.

8 Um die ftp-Verbindung zu schließen, geben Sie bye ein.

```
ftp> bye
```

Beispiel 29–7 Kopieren von Dateien in ein Remote-System (ftp)

In diesem Beispiel öffnet der Benutzer kryten eine ftp-Verbindung mit dem System pluto und verwendet den Befehl put, um eine Datei aus seinem System in das /tmp-Verzeichnis auf dem System pluto zu kopieren.

```
$ cd /tmp
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> put filef
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34357) (0 bytes).
filea
filef
files
ps_data
226 ASCII Transfer complete.
60 bytes received in 0.058 seconds (1.01 Kbytes/s)
ftp> bye
221 Goodbye.
```

In diesem Beispiel verwendet der Benutzer kryten den Befehl mput, um Dateien aus seinem Home-Verzeichnis in das pluto-Verzeichnis /tmp zu kopieren. Beachten Sie, dass der Benutzer kryten die Möglichkeit hat, einzelne Dateien zu akzeptieren oder abzulehnen.

```
$ cd $HOME/testdir
$ ls
test1   test2   test3
$ ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> mput test*
mput test1? y
200 PORT command successful.
150 ASCII data connection for test1 (129.152.221.238,34365).
226 Transfer complete.
mput test2? y
200 PORT command successful.
150 ASCII data connection for test2 (129.152.221.238,34366).
226 Transfer complete.
mput test3? y
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> bye
221 Goodbye.
```

Remote-Kopieren mit rcp

Mithilfe des Befehls rcp werden Dateien oder Verzeichnisse zwischen einem lokalen System und einem Remote-System oder zwischen zwei Remote-Systemen kopiert. Sie können diesen Befehl von einem Remote-System aus (nachdem Sie sich mit dem Befehl rlogin angemeldet haben) oder vom lokalen System aus (ohne sich bei einem Remote-System anzumelden) verwenden.

Mit rcp können Sie die folgenden Remote-Kopiervorgänge ausführen:

- Kopieren einer Datei oder eines Verzeichnisses von Ihrem System auf ein Remote-System
- Kopieren einer Datei oder eines Verzeichnisses von einem Remote-System auf Ihr lokales System
- Kopieren einer Datei oder eines Verzeichnisses von Ihrem lokalen System zwischen Remote-Systemen

Wenn der Automounter ausgeführt wird, können Sie diese Vorgänge mit dem Befehl cp ausführen. Jedoch ist die Geltung von cp auf das vom Automounter erstellte virtuelle

Dateisystem beschränkt, sowie auf Vorgänge, die das Home-Verzeichnis eines Benutzers betreffen. Da von rcp dieselben Vorgänge ohne diese Beschränkungen ausgeführt werden, werden in diesem Abschnitt nur die rcp-Varianten dieser Aufgaben beschrieben.

Sicherheitsüberlegungen für Kopiervorgänge

Um Dateien oder Verzeichnisse zwischen Systemen zu kopieren, müssen Sie über die Berechtigungen zum Anmelden und zum Kopieren von Dateien verfügen.

Achtung – Sowohl mit dem Befehl cp als auch mit dem Befehl rcp können Dateien ohne Warnung überschrieben werden. Stellen Sie sicher, dass die Dateinamen richtig sind, bevor Sie den Befehl ausführen.

Angeben von Quelle und Ziel

Mit dem Befehl rcp in der C-Shell können Sie die Quelle (die Datei oder das Verzeichnis, das kopiert werden soll) und das Ziel (die Stelle, an die Sie die Datei oder das Verzeichnis kopieren) angeben. Dazu verwenden Sie entweder einen absoluten oder abgekürzten Pfadnamen.

	Absolute Pfadnamen	Abgekürzte Pfadnamen
Vom lokalen System	`mars:/home/jones/myfile.txt`	`~jones/myfile.txt`
Nach der Remote-Anmeldung	`/home/jones/myfile.txt`	`~jones/myfile.txt`

Absolute Pfadnamen dienen zur Kennzeichnung von Dateien oder Verzeichnisse, die auf einem bestimmten System eingehängt sind. Im vorangegangenen Beispiel kennzeichnet der erste absolute Pfadname eine Datei (`myfile.txt`) auf dem System `mars`. Abgekürzte Pfadnamen kennzeichnen Dateien oder Verzeichnisse in Relation zu einem Home-Verzeichnis eines Benutzers, egal wo sich dieses Verzeichnis befindet. Im vorangegangenen ersten Beispiel wird dieselbe Datei (`myfile.txt`) durch den Pfadnamen gekennzeichnet, aber es wird eine Tilde (~) verwendet, um das `jones`-Home-Verzeichnis anzugeben:

```
~ = mars:/home/jones
```

Die Beispiele in der zweiten Zeile zeigen einen Benutzer, der nach einer Remote-Anmeldung absolute und abgekürzte Pfadnamen verwendet. Es ist kein Unterschied ersichtlich, was den abgekürzten Pfadnamen anbetrifft. Da jedoch durch die Remote-Anmeldung das `jones`-Home-Verzeichnis auf dem lokalen System (parallel zum Home-Verzeichnis des lokalen Benutzers) eingehängt wurde, wird der Systemname `mars` nicht mehr für den absoluten Pfad

benötigt. Weitere Informationen darüber, wie durch eine Remote-Anmeldung ein anderes Home-Verzeichnis eines Benutzers eingehängt wird, finden Sie unter „Vorgang nach der Remote-Anmeldung“ auf Seite 684.

Die folgende Tabelle enthält ein Beispiel für absolute und abgekürzte Pfadnamen, die von der C-Shell erkannt werden. Im Beispiel wird die folgende Terminologie verwendet:

- Arbeitsverzeichnis – das Verzeichnis, von dem aus der Befehl `rcp` eingegeben wird. Es kann sich um ein Remote-Verzeichnis oder ein lokales Verzeichnis handeln.
- Aktueller Benutzer – der Benutzername, unter dem der Befehl `rcp` eingegeben wird.

TABELLE 29–4 Zulässige Syntaxen für Verzeichnis- und Dateinamen

Angemeldet bei	Syntax	Beschreibung
Lokales System	.	Das lokale Arbeitsverzeichnis
	path/filename	Der Pfad (*path*) und der Dateiname (*path*) im lokalen Arbeitsverzeichnis
	~	Das Home-Verzeichnis des aktuellen Benutzers
	~/path/filename	Der Pfad (*path*) und der Dateiname (*filename*) unter dem Home-Verzeichnis des aktuellen Benutzers
	~user	Das Home-Verzeichnis des Benutzers (*user*)
	~user/path/filename	Der Pfad (*path*) und der Dateiname (*filename*) unter dem Home-Verzeichnis des *Benutzers*
	remote-system:path/filename	Der Pfad (*path*) und der Dateiname (*filename*) im Remote-Arbeitsverzeichnis
Remote-System	.	Das Remote-Arbeitsverzeichnis
	filename	Der Dateiname (*filename*) im Remote-Arbeitsverzeichnis
	path/filename	Der Pfad (*path*) und der Dateiname (*filename*) im Remote-Arbeitsverzeichnis
	~	Das Home-Verzeichnis des aktuellen Benutzers
	~/path/filename	Der Pfad (*path*) und der Dateiname (*filename*) im Home-Verzeichnis des aktuellen Benutzers
	~user	Das Home-Verzeichnis des Benutzers (*user*)
	~/user/path/filename	Der Pfad (*path*) und der Dateiname (*filename*) unter dem Home-Verzeichnis des *Benutzers*
	local-system:path/filename	Der Pfad (*path*) und der Dateiname (*path*) im lokalen Arbeitsverzeichnis

▼ So kopieren Sie Dateien zwischen einem lokalen System und einem Remote-System (rcp)

1 Stellen Sie sicher, dass Sie über eine Berechtigung zum Kopieren verfügen.

Sie sollten zumindest über eine Leseberechtigung für das Quellsystem und eine Schreibberechtigung für das Zielsystem verfügen.

2 Bestimmen Sie den Speicherort der Quelle und des Ziels.

Wenn Sie den Pfad der Quelle oder des Ziels nicht kennen, melden Sie sich zunächst beim Remote-System an, indem Sie den Befehl `rlogin` ausführen. Informationen zur Vorgehensweise finden Sie unter „So melden Sie sich bei einem Remote-System an (rlogin)“ auf Seite 687. Anschließend navigieren Sie durch das Remote-System, bis Sie den Speicherort gefunden haben. Dann führen Sie den nächsten Schritt aus, ohne sich abzumelden.

3 Kopieren Sie die Datei oder das Verzeichnis.

`$ rcp [-r]` *source-file|directory target-file|directory*

`rcp` (Keine Optionen) Kopiert eine einzelne Datei aus der Quelle in das Ziel.

`-r` Kopiert ein Verzeichnis aus der Quelle in das Ziel.

Diese Syntax gilt unabhängig davon, ob Sie beim Remote-System oder beim lokalen System angemeldet sind. Nur der Pfadname der Datei oder des Verzeichnisses wird geändert, wie in Tabelle 29–4 beschrieben und in den folgenden Beispielen erläutert.

Sie können die Tilde (~) und den Punkt (`.`) verwenden, um die Pfadteile des Namens der lokalen Datei oder des Verzeichnisnamens anzugeben. Beachten Sie jedoch, dass die Tilde (~) für den aktuellen Benutzer gilt, nicht aber für das Remote-System, und dass der Punkt (`.`) für das System gilt, bei dem Sie angemeldet sind. Erläuterungen dieser Symbolle finden Sie in Tabelle 29–4.

Beispiel 29–8 Verwenden von `rcp`, um eine Remote-Datei auf ein lokales System zu kopieren

In diesem Beispiel wird `rcp` verwendet, um die Datei `letter.doc` aus dem `/home/jones`-Verzeichnis des Remote-Systems `pluto` in das Arbeitsverzeichnis (`/home/smith`) auf dem lokalen System (`earth`) zu kopieren:

```
earth(/home/smith): rcp pluto:/home/jones/letter.doc .
```

In diesem Fall wird der `rcp`-Vorgang ohne Remote-Anmeldung durchgeführt. Hier bezieht sich der Punkt (`.`) am Ende der Befehlszeile auf das lokale System und nicht auf das Remote-System.

Da das Zielverzeichnis gleichzeitig das Home-Verzeichnis des lokalen Benutzers ist, kann es mit der Tilde (~) angegeben werden.

Beispiel 29–9 Verwenden von rlogin und rcp, um eine Remote-Datei in ein lokales System zu kopieren

In diesem Beispiel wird der rcp-Vorgang ausgeführt, nachdem der Befehl rlogin ausgeführt wurde, um eine Datei aus einem Remote-System in ein lokales System zu kopieren. Obwohl der Ablauf des Vorgangs derselbe wie im vorangegangenen Beispiel ist, werden die Pfade verändert, um die Remote-Anmeldung zu ermöglichen:

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp letter.doc ~
```

Die Verwendung des Punkts (.) am Ende der Befehlszeile wäre in diesem Fall nicht angebracht. Da es sich um eine Remote-Anmeldung handelt, wäre der Punkt ein Verweis auf das Remote-System, wodurch rcp eine duplizierte Datei erstellen würde. Die Tilde (~) jedoch bezieht sich auf das Home-Verzeichnis des aktuellen Benutzers, was auch dann der Fall ist, wenn die Anmeldung bei einem Remote-System stattfindet.

Beispiel 29–10 Verwenden von rcp, um eine lokale Datei in ein Remote-System zu kopieren

In diesem Beispiel wird rcp verwendet, um die Datei notice.doc aus dem Home-Verzeichnis (/home/smith) des lokalen Systems earth in das /home/jones-Verzeichnis des Remote-Systems pluto zu kopieren:

```
earth(/home/smith): rcp notice.doc pluto:/home/jones
```

Da kein Name der Remote-Datei angegeben ist, wird die Datei notice.doc mit dem gleichen Namen in das /home/jones-Verzeichnis kopiert.

In diesem Fall wird der im vorangegangenen Beispiel aufgeführte rcp-Vorgang wiederholt, aber auf rcp wird aus einem anderen Arbeitsverzeichnis auf dem lokalen System (/tmp) zugegriffen. Beachten Sie, dass sich die Tilde (~) auf das Home-Verzeichnis des aktuellen Benutzers bezieht:

```
earth(/tmp): rcp ~/notice.doc pluto:/home/jones
```

Beispiel 29–11 Verwenden von rlogin und rcp, um eine lokale Datei auf ein Remote-System zu kopieren

In diesem Beispiel wird der rcp-Vorgang ausgeführt, nachdem der Befehl rlogin ausgeführt wurde, um eine lokale Datei in ein Remote-Verzeichnis zu kopieren. Obwohl der Ablauf des Vorgangs derselbe wie im vorangegangenen Beispiel ist, werden die Pfade verändert, um die Remote-Anmeldung zu ermöglichen.

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp ~/notice.doc .
```

In diesem Fall kann die Tilde (~) verwendet werden, um das Home-Verzeichnis des aktuellen Benutzers zu benennen, obwohl sich das Verzeichnis auf dem lokalen System befindet. Der Punkt (.) bezieht sich auf das Arbeitsverzeichnis auf dem Remote-System, weil der Benutzer beim Remote-System angemeldet ist. Dies ist eine alternative Syntax für die Ausführung desselben Vorgangs:

```
pluto(/home/jones): rcp earth:/home/smith/notice.doc /home/jones
```

TEIL VII

Überwachen von Netzwerkdiensten – Themen

Dieser Abschnitt enthält schrittweise Anweisungen zum Überwachen von Netzwerkdiensten.

◆ ◆ ◆ KAPITEL 30

Überwachen der Netzwerkleistung (Aufgaben)

In diesem Kapitel wird beschrieben, wie die Netzwerkleistung überwacht wird. Im Folgenden sind die schrittweisen Anleitungen in diesem Kapitel aufgeführt.

- „So prüfen Sie die Antwort von Hosts im Netzwerk“ auf Seite 704
- „So senden Sie Pakete an Hosts im Netzwerk“ auf Seite 704
- „So erfassen Sie Pakete aus dem Netzwerk“ auf Seite 705
- „So prüfen Sie den Netzwerkstatus“ auf Seite 705
- „So zeigen Sie NFS-Server- und -Clientstatistiken an“ auf Seite 708

Überwachen der Netzwerkleistung

In Tabelle 30–1 werden die Befehle aufgeführt, die zur Verfügung stehen, um die Netzwerkleistung zu überwachen.

TABELLE 30–1 Befehle zur Überwachung des Netzwerks

Befehl	Beschreibung
`ping`	Prüft die Antwort von Hosts im Netzwerk.
`spray`	Prüft die Zuverlässigkeit Ihrer Paketgrößen. Dieser Befehl kann Ihnen mitteilen, ob die Übermittlung von Paketen im Netzwerk verzögert wird oder Pakete abgeworfen werden.
`snoop`	Erfasst aus dem Netzwerk kommende Pakete und verfolgt die Aufrufe, die von jedem Client an jeden Server gesendet werden.
`netstat`	Zeigt den Netzwerkstatus an sowie den Status der Schnittstellen, die für den TCP/IP-Verkehr verwendet werden, die IP-Routing-Tabelle und die pro Protokoll geführten Statistiken für `UDP`, `TCP`, `ICMP` und `IGMP`.
`nfsstat`	Zeigt eine Zusammenfassung der Server- und Clientstatistiken an, die verwendet werden können, um NFS-Probleme zu erkennen.

So prüfen Sie die Antwort von Hosts im Netzwerk

Prüfen Sie die Antwort von Hosts im Netzwerk, indem Sie den Befehl `ping` verwenden.

`$` **`ping`** *hostname*

Wenn Sie ein physisches Problem vermuten, können Sie `ping` verwenden, um die Antwortzeiten von mehreren Hosts im Netzwerk zu prüfen. Wenn die Antwort von einem Host nicht wie erwartet ausfällt, können Sie diesen Host untersuchen. Physische Probleme können folgende Ursachen haben:

- Lockere Kabel oder Verbindungen
- Falsche Erdung
- Kein Abschluss
- Signalreflexion

Weitere Informationen zu diesem Befehl finden Sie unter `ping(1M)`.

BEISPIEL 30–1 Prüfen der Antwort von Hosts im Netzwerk

Die einfachste Version von `ping` sendet ein einzelnes Paket an einen Host im Netzwerk. Wenn `ping` die richtige Antwort erhält, gibt der Befehl die Meldung *host* `is alive` aus.

```
$ ping elvis
elvis is alive
```

Mit der Option `-s` sendet `ping` ein Datagramm pro Sekunde an einen Host. Anschließend gibt der Befehl die jeweiligen Antworten aus, sowie die Zeiten, die für den gesamten Vorgang benötigt wurden. Ein Beispiel:

```
$ ping -s pluto
64 bytes from pluto (123.456.78.90): icmp_seq=0. time=3.82 ms
64 bytes from pluto (123.456.78.90): icmp_seq=5. time=0.947 ms
64 bytes from pluto (123.456.78.90): icmp_seq=6. time=0.855 ms
^C
----pluto PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss

round-trip (ms) min/avg/max/sttdev = 0.855/1.87/3.82/1.7
```

So senden Sie Pakete an Hosts im Netzwerk

Prüfen Sie die Zuverlässigkeit Ihrer Paketgrößen mit dem Befehl `spray`.

`$` **`spray`** `[ -c` *count* `-d` *interval* `-l` *packet-size*`]` *hostname*

`-i` *count* Anzahl der Pakete, die gesendet werden sollen.

`-d` *interval*	Anzahl von Mikrosekunden zum Unterbrechen zwischen dem Senden von Paketen. Wenn Sie keine Verzögerung verwenden, können die Puffer überlastet werden.
`-l` *packet-size*	Die Paketgröße.
hostname	Das System, an das Pakete gesendet werden.

Weitere Informationen zu diesem Befehl finden Sie unter `spray(1M)`.

BEISPIEL 30–2 Senden von Paketen an Hosts im Netzwerk

Im folgenden Beispiel werden 100 Pakete an einen Host (`-c 100`) gesendet. Die Paketgröße beträgt 2048 Byte (`-l 2048`). Die Pakete werden mit einer Verzögerung von 20 Mikrosekunden zwischen jedem Burst gesendet (`-d 20`).

```
$ spray -c 100 -d 20 -l 2048 pluto
sending 100 packets of length 2048 to pluto ...
no packets dropped by pluto
279 packets/sec, 573043 bytes/sec
```

So erfassen Sie Pakete aus dem Netzwerk

Um Pakete aus dem Netzwerk zu erfassen und die einzelnen Clientaufrufe der jeweiligen Server zu verfolgen, verwenden Sie `snoop`. Dieser Befehl stellt genaue Zeitstempel bereit, mit deren Hilfe manche Netzwerkprobleme rasch isoliert werden können. Weitere Informationen finden Sie unter `snoop(1M)`.

```
# snoop
```

Abgeworfene Pakete können auf zu wenig Pufferspeicher oder eine überlastete CPU zurückgeführt werden.

So prüfen Sie den Netzwerkstatus

Um Informationen über Netzwerkstatus wie beispielsweise Statistiken zum Status von Netzwerkschnittstellen, Routing-Tabellen und verschiedene Protokolle anzuzeigen, verwenden Sie den Befehl `netstat`.

```
$ netstat [-i] [-r] [-s]
```

`-i` Zeigt den Status der TCP/IP-Schnittstellen an.

`-r` Zeigt die IP-Routing-Tabelle an.

`-s` Zeigt Statistiken für die `UDP`-, `TCP`-, `ICMP`- und `IGMP`-Protokolle an.

Weitere Informationen finden Sie unter netstat(1M).

Prüfen des Netzwerkstatus – Beispiele

Das folgende Beispiel zeigt eine Ausgabe des Befehls `netstat -i`, der den Status der Schnittstellen anzeigt, die für TCP/IP-Verkehr verwendet werden.

```
$ netstat -i
Name  Mtu  Net/Dest    Address      Ipkts  Ierrs Opkts  Oerrs Collis Queue
lo0   8232 software    localhost     1280   0     1280     0       0    0
eri0   1500 loopback    venus      1628480   0   347070    16   39354    0
```

Diese Ausgabe zeigt die Anzahl der Pakete an, die ein Rechner übertragen und über jede Schnittstelle empfangen hat. Ein Rechner mit aktivem Netzwerkverkehr sollte einen kontinuierlichen Anstieg von sowohl `Ipkts` als auch `Opkts` aufweisen.

Berechnen Sie die Kollisionsquote des Netzwerks, indem Sie die Anzahl der Kollisionen (`Collis`) durch die Anzahl der Pakete (`Opkts`) dividieren. Im vorangegangenen Beispiel beträgt die Kollisionsquote 11 Prozent. Eine netzwerkübergreifende Kollisionsquote, die über 5 bis 10 Prozent liegt, kann auf ein Problem hindeuten.

Berechnen Sie die Fehlerquote der Eingangspakete, indem Sie die Anzahl der Eingangsfehler durch die Gesamtanzahl der Eingangspakete (`Ierrs/Ipkts`) dividieren. Die Fehlerquote der Ausgangspakete ergibt sich aus der Anzahl der Ausgangsfehler, die durch die Gesamtanzahl der Ausgangspakete (`Oerrs/Opkts`) dividiert wird. Wenn die Eingangsfehlerquote hoch ist, d. h. über 0,25 Prozent, wirft der Host möglicherweise Pakete ab.

Das folgende Beispiel zeigt die Ausgabe des Befehls `netstat -s`, der die pro Protokoll geführten Statistiken für die `UDP`-, `TCP`-, `ICMP`- und `IGMP`-Protokolle anzeigt.

```
UDP
    udpInDatagrams      =196543    udpInErrors         =     0
    udpOutDatagrams     =187820

TCP
    tcpRtoAlgorithm     =     4    tcpRtoMin           =   200
    tcpRtoMax           = 60000    tcpMaxConn          =    -1
    tcpActiveOpens      = 26952    tcpPassiveOpens     =   420
    tcpAttemptFails     =  1133    tcpEstabResets      =     9
    tcpCurrEstab        =    31    tcpOutSegs          =3957636
    tcpOutDataSegs      =2731494   tcpOutDataBytes     =1865269594
    tcpRetransSegs      = 36186    tcpRetransBytes     =3762520
    tcpOutAck           =1225849   tcpOutAckDelayed    =165044
    tcpOutUrg           =     7    tcpOutWinUpdate     =   315
    tcpOutWinProbe      =     0    tcpOutControl       = 56588
    tcpOutRsts          =   803    tcpOutFastRetrans   =   741
    tcpInSegs           =4587678
    tcpInAckSegs        =2087448   tcpInAckBytes       =1865292802
    tcpInDupAck         =109461    tcpInAckUnsent      =     0
    tcpInInorderSegs    =3877639   tcpInInorderBytes   =-598404107
    tcpInUnorderSegs    = 14756    tcpInUnorderBytes   =17985602
```

```
    tcpInDupSegs        =    34    tcpInDupBytes       = 32759
    tcpInPartDupSegs    =   212    tcpInPartDupBytes   =134800
    tcpInPastWinSegs    =     0    tcpInPastWinBytes   =     0
    tcpInWinProbe       =   456    tcpInWinUpdate      =     0
    tcpInClosed         =    99    tcpRttNoUpdate      =  6862
    tcpRttUpdate        =435097    tcpTimRetrans       = 15065
    tcpTimRetransDrop   =    67    tcpTimKeepalive     =   763
    tcpTimKeepaliveProbe=     1    tcpTimKeepaliveDrop =     0

IP
    ipForwarding        =     2    ipDefaultTTL        =   255
    ipInReceives        =11757234  ipInHdrErrors       =     0
    ipInAddrErrors      =     0    ipInCksumErrs       =     0
    ipForwDatagrams     =     0    ipForwProhibits     =     0
    ipInUnknownProtos   =     0    ipInDiscards        =     0
    ipInDelivers        =4784901   ipOutRequests       =4195180
    ipOutDiscards       =     0    ipOutNoRoutes       =     0
    ipReasmTimeout      =    60    ipReasmReqds        =  8723
    ipReasmOKs          =  7565    ipReasmFails        =  1158
    ipReasmDuplicates   =     7    ipReasmPartDups     =     0
    ipFragOKs           = 19938    ipFragFails         =     0
    ipFragCreates       =116953    ipRoutingDiscards   =     0
    tcpInErrs           =     0    udpNoPorts          =6426577
    udpInCksumErrs      =     0    udpInOverflows      =   473
    rawipInOverflows    =     0

ICMP
    icmpInMsgs          =490338    icmpInErrors        =     0
    icmpInCksumErrs     =     0    icmpInUnknowns      =     0
    icmpInDestUnreachs  =   618    icmpInTimeExcds     =   314
    icmpInParmProbs     =     0    icmpInSrcQuenchs    =     0
    icmpInRedirects     =   313    icmpInBadRedirects  =     5
    icmpInEchos         =   477    icmpInEchoReps      =    20
    icmpInTimestamps    =     0    icmpInTimestampReps =     0
    icmpInAddrMasks     =     0    icmpInAddrMaskReps  =     0
    icmpInFragNeeded    =     0    icmpOutMsgs         =   827
    icmpOutDrops        =   103    icmpOutErrors       =     0
    icmpOutDestUnreachs =    94    icmpOutTimeExcds    =   256
    icmpOutParmProbs    =     0    icmpOutSrcQuenchs   =     0
    icmpOutRedirects    =     0    icmpOutEchos        =     0
    icmpOutEchoReps     =   477    icmpOutTimestamps   =     0
    icmpOutTimestampReps=     0    icmpOutAddrMasks    =     0
    icmpOutAddrMaskReps =     0    icmpOutFragNeeded   =     0
    icmpInOverflows     =     0

IGMP:
        0 messages received
        0 messages received with too few bytes
        0 messages received with bad checksum
        0 membership queries received
        0 membership queries received with invalid field(s)
        0 membership reports received
        0 membership reports received with invalid field(s)
        0 membership reports received for groups to which we belong
        0 membership reports sent
```

Im folgenden Beispiel wird eine Ausgabe des Befehls `netstat - r` gezeigt, der die IP-Routing-Tabelle anzeigt.

```
Routing Table:
  Destination        Gateway           Flags  Ref   Use    Interface
------------------ -------------------- ----- ----- ------ ---------
localhost          localhost             UH       0   2817  lo0
earth-bb           pluto                 U        3  14293  eri0
224.0.0.0          pluto                 U        3      0  eri0
default            mars-gate             UG       0  14142
```

Die Felder im `netstat - r`-Bericht werden in folgender Tabelle beschrieben.

TABELLE 30–2 Ausgabe des Befehls `netstat - r`

Feldname		Beschreibung
`Flags`	`U`	Die Route ist aktiviert.
	`G`	Die Route führt durch ein Gateway.
	`H`	Die Route führt zu einem Host.
	`D`	Die Route wurde mithilfe einer Umleitung dynamisch erstellt.
`Ref`		Zeigt die aktuelle Anzahl von Routen an, die dieselbe Sicherungsschicht verwenden.
`Use`		Zeigt die Anzahl der gesendeten Pakete an.
`Interface`		Listet die Netzwerkschnittstelle auf, die für die Route verwendet wird.

So zeigen Sie NFS-Server- und -Clientstatistiken an

Der NFS-Distributed File Service verwendet einen Remote-Prozeduraufruf (Remote Procedure Call, RPC), der lokale Befehle in Aufrufe für den Remote-Host umsetzt. Die Remote-Prozeduraufrufe werden synchron durchgeführt. Die Clientanwendung wird gesperrt oder ausgesetzt, bis der Server den Aufruf durchgeführt und die Ergebnisse zurückgegeben hat. Einer der wichtigsten Faktoren, die Einfluss auf die NFS-Leistung haben, ist die Neuübertragungsrate.

Wenn der Dateiserver nicht auf den Aufruf eines Clients antworten kann, sendet der Client den Aufruf erneut. Stellt sich nach einer bestimmten Anzahl von Sendeversuchen kein Erfolg ein, bricht der Client den Vorgang ab. Jede Neuübertragung erhöht den Systemaufwand und den Netzwerkverkehr. Übermäßig viele Neuübertragungen können die Netzwerkleistung beeinträchtigen. Wenn die Neuübertragungsrate zu hoch ist, sollten Sie prüfen, ob einer der folgenden Zustände gegeben ist:

- Zu langsame Verarbeitung von Aufrufen durch überlastete Server
- Eine Ethernet-Schnittstelle wirft Pakete ab
- Verlangsamte Paketübertragung durch Netzwerküberlastung

In folgender Tabelle werden die `nfsstat`-Optionen beschrieben, die zum Anzeigen von Client- und Serverstatistiken dienen.

TABELLE 30–3 Befehle zum Anzeigen von Client- und Serverstatistiken

Befehl	Anzeige
`nfsstat -c`	Clientstatistiken
`nfsstat -s`	Serverstatistiken
`netstat -m`	Netzwerkstatistiken für jedes Dateisystem

Verwenden Sie `nfsstat -c`, um Clientstatistiken anzuzeigen, und `nfsstat -s`, um Serverstatistiken anzuzeigen. Verwenden Sie `netstat -m`, um Netzwerkstatistiken für jedes Dateisystem anzuzeigen. Weitere Informationen finden Sie unter `nfsstat(1M)`.

Anzeigen von NFS-Server- und -Clientstatistiken – Beispiele

Im folgenden Beispiel werden RPC- und NFS-Daten für den Client `pluto` gezeigt.

```
$ nfsstat -c

Client rpc:
Connection oriented:
calls    badcalls  badxids  timeouts newcreds  badverfs   timers
1595799  1511      59       297      0         0          0
cantconn nomem     interrupts
1198      0         7
Connectionless:
calls    badcalls  retrans  badxids  timeouts  newcreds   badverfs
80785    3135      25029    193      9543      0          0
timers   nomem     cantsend
17399    0         0

Client nfs:
calls    badcalls  clgets   cltoomany
1640097  3112      1640097  0
Version 2: (46366 calls)
null     getattr   setattr  root     lookup     readlink  read
```

```
0 0%     6589 14%  2202 4%  0 0%     11506 24%  0 0%      7654 16%
wrcache  write     create   remove   rename     link      symlink
0 0%     13297 28% 1081 2%  0 0%     0 0%       0 0%      0 0%
mkdir    rmdir     readdir  statfs
24 0%    0 0%      906 1%   3107 6%
Version 3: (1585571 calls)
null    getattr    setattr  lookup     access     readlink  read
0 0%    508406 32% 10209 0% 263441 16% 400845 25% 3065 0%  117959 7%
write    create     mkdir    symlink    mknod    remove   rmdir
69201 4% 7615 0%    42 0%    16 0%      0 0%     7875 0%  51 0%
rename   link       readdir  readdir+   fsstat   fsinfo   pathconf
929 0%   597 0%     3986 0%  185145 11% 942 0%   300 0%   583 0%
commit
4364 0%

Client nfs_acl:
Version 2: (3105 calls)
null       getacl     setacl     getattr    access
0 0%       0 0%       0 0%       3105 100%  0 0%
Version 3: (5055 calls)
null       getacl     setacl
0 0%       5055 100%  0 0%
```

Die Ausgabe des Befehls `nfsstat -c` wird in folgender Tabelle beschrieben.

TABELLE 30–4 Ausgabe des Befehls `nfsstat -c`

Feld	Beschreibung
`calls`	Die Gesamtanzahl der gesendeten Aufrufe
`badcalls`	Die Gesamtanzahl der Aufrufe, die von RPC abgewiesen wurden
`retrans`	Die Häufigkeit der Neuübertragungen. Für diesen Client liegt die Neuübertragungsrate bei weniger als einem Prozent. Dies entspricht etwa 10 Zeitüberschreitungen bei 6888 Aufrufen. Diese Neuübertragungen können zeitweilige Ausfälle verursachen. Höhere Raten können auf ein Problem hindeuten.
`badxid`	Die Häufigkeit des Empfangs einer duplizierten Bestätigung für einen einzelnen NFS-Aufruf
`timeout`	Die Häufigkeit von Zeitüberschreitungen bei Aufrufen
`wait`	Die Häufigkeit des Wartens eines Aufrufs, weil kein Client-Handle verfügbar war
`newcred`	Die Häufigkeit der notwendigen Aktualisierungen von Authentifizierungsinformationen
`timers`	Die Häufigkeit von Zeitüberschreitungen, deren Wert größer oder ebenso groß wie der angegebene Zeitüberschreitungswert für einen Aufruf ist
`readlink`	Die Häufigkeit, mit der ein Lesevorgang (`read`) für eine symbolische Verknüpfung ausgeführt wurde. Wenn diese Zahl hoch ist, d. h. höher als 10 Prozent, sind möglicherweise zu viele symbolische Verknüpfungen vorhanden.

Im folgenden Beispiel wird die Ausgabe des Befehls `nfsstat -m` angezeigt:

```
pluto$ nfsstat -m
/usr/man from pluto:/export/svr4/man
Flags: vers=2,proto=udp,auth=unix,hard,intr,dynamic,
        rsize=8192, wsize=8192,retrans=5
 Lookups: srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
 All:     srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
```

Die Ausgabe des Befehls `nfsstat -m`, die in Millisekunden angezeigt wird, wird in folgender Tabelle beschrieben.

TABELLE 30–5 Ausgabe des Befehls `nfsstat -m`

Feld	Beschreibung
`srtt`	Der geglättete Mittelwert von Round-Trip-Zeiten
`dev`	Die durchschnittlichen Abweichungen
`cur`	Die derzeit "erwartete" Antwortzeit

Wenn Sie vermuten, dass die Hardwarekomponenten Ihres Netzwerks Probleme verursachen, führen Sie eine gründliche Untersuchung der Verkabelungen und Verbindungen durch.

Glossar

asppp — Eine Version des PPP, die in die Versionen 2.4 bis 8 des Betriebssystems Solaris aufgenommen wurde. `asppp` unterstützte nur die asynchrone PPP-Kommunikation.

asynchrones PPP — Ein PPP, das über asynchrone serielle Zeilen läuft, die jeweils ein Zeichen von Daten übertragen. Die am häufigsten verwendete Form der PPP-Konfiguration, die Wählverbindung, verwendet die asynchrone PPP-Kommunikation.

Authentifizierung — Die Verifizierung der Identität über das Netzwerk über einen Remote-Benutzer oder eine Entität wie beispielsweise ein Programm. Manche Authentifizierungsprotokolle ermöglichen, Datenbanken mit Authentifizieruns-Berechtigungsnachweisen von potenziellen Benutzern einzurichten. Andere Authentifizierungsprotokolle verwenden vertrauenswürdige Zertifikatsketten, die von einer Zertifizierungsstelle für Authentifizierungszwecke ausgegeben werden. Diese Berechtigungsnachweise können Benutzer authentifizieren, wenn diese versuchen, mit Ihnen zu kommunizieren oder die Services Ihrer Site zu verwenden.

Benutzeragent (User Agent, UA) — Der SLP-Agent, der im Auftrag der Benutzeranwendung handelt. Der Agent fordert die Identität der entsprechenden Bereiche, Verzeichnisagenten und Service-Advertisements an.

Bereich — Eine Gruppe von UAs und SAs, die administrativ, topologisch oder auf andere Art angeordnet ist. Sie können Bereiche verwenden, um festzulegen bzw. zu ändern, wie Sie den Zugriff auf Services im Unternehmen bereitstellen.

Broadcast — Ein Sicherungsschichtverfahren, das verwendet wird, um Pakete an jeden Rechner in einem Teilnetz zu übermitteln. Broadcast-Pakete werden normalerweise nicht über das Teilnetz hinaus weitergeleitet.

CBCP (Callback Control Protocol) — Eine proprietäre Microsoft-PPP-Erweiterung, die verwendet wird, um eine Callback-Sitzung auszuhandeln. Solaris PPP 4.0 unterstützt nur die Clientseite (das anfangs aufrufende Programm) dieses Protokolls.

CCP (Compression Control Protocol) — Ein Unterprotokoll des PPP, das die Verwendung der Datenkomprimierung für die Verbindung aushandelt. Anders als bei der Header-Komprimierung komprimiert CCP alle Daten innerhalb von Paketen, die über die Verbindung gesendet werden.

CHAP

Das CHAP (Challenge-Handshake Authentication Protocol) ist ein Authentifizierungsprotokoll, das verwendet werden kann, um die Identität eines aufrufenden Programms über eine PPP-Verbindung zu verifizieren. Bei der CHAP-Authentifizierung wird das Konzept der *Aufforderung* und *Antwort* verwendet. Bei diesem Konzept wird durch den Rechner, der einen Aufruf empfängt, das aufrufende Programm aufgefordert, seine Identität nachzuweisen.

Siehe auch PAP (Password Authentication Protocol).

CHAP-Geheimnis

Eine ASCII- oder Binärzeichenfolge, die für Identifizierungszwecke verwendet wird und beiden Peers in einer PPP-Verbindung bekannt ist. Das CHAP-Geheimnis wird in Klartext in einer `/etc/ppp/chap-secrets`-Systemdatei gespeichert, aber nie über die PPP-Verbindung gesendet, nicht einmal in verschlüsselter Form. Das CHAP-Protokoll verifiziert, dass ein Hashcode des CHAP-Geheimnisses, das von einem aufrufenden Programm verwendet wird, mit einem Hashcode des CHAP-Geheimniseintrags für das aufrufende Programm in der `/etc/ppp/chap-secrets`-Datei des Empfängers übereinstimmt.

Chat-Skript

Anweisungen, die einem Modem mitteilen, wie eine Kommunikationsverbindung zwischen dem Modem selbst und einem Remote-Peer hergestellt wird. Sowohl die PPP- als auch die UUCP-Protokolle verwenden Chat-Skripten, um Wählverbindungen und Rückrufverbindungen aufzubauen.

CSU (Channel Service Unit)

Die Servicekanaleinheit (CSU) ist ein synchrones Telekommunikationsgerät, das eine lokale Schnittstelle zu einer Telekommunikationsstandleitung bereitstellt und diese Leitung abschließt. In den USA schließt eine CSU eine T1-Leitung ab und stellt ein DS1 oder eine DSX-Schnittstelle bereit. International ist die CSU normalerweise im Besitz der Telefongesellschaft.

Siehe auch CSU/DSU und Data Service Unit (DSU).

CSU/DSU

Ein synchrones Telekommunikationsgerät, das CSU- und DSU-Geräte kombiniert und für eine PPP-Standleitungsverbindung verwendet wird. Das CSU/DSU-Gerät überträgt Signale von einem Peer in eine Standleitung. Die meisten CSU/DSUs benötigen kein Chat-Skript, um eine Verbindung herzustellen. CSU/DSUs werden oft vom Anbieter der Standleitung konfiguriert.

Siehe auch CSU (Channel Service Unit) und Data Service Unit (DSU).

Data Service Unit (DSU)

Die Servicedateneinheit (DSU) ist ein synchrones Telekommunikationsgerät, das für eine PPP-Standleitungsverbindung verwendet wird. Die DSU führt Konvertierungen zwischen Daten-Framing-Formaten durch, die für Telekommunikationsleitungen verwendet werden, und stellt eine Kommunikationsschnittstelle für Standarddaten bereit.

Siehe auch CSU (Channel Service Unit) und CSU/DSU.

Einwahlserver Der Peer, der den Empfänger einer PPP-Wählverbindung aushandelt und festlegt, nachdem ein Anruf von einem Hinauswahlrechner eingegangen ist. Obwohl der Begriff "Einwahlserver" allgemein verwendet wird, funktioniert ein Einwahlserver nicht wie ein Client-Server-Paradigma. Er ist vielmehr der Peer, der antwortet, wenn der Aufbau einer Wählverbindung angefordert wird. Sobald ein Einwahlserver konfiguriert ist, kann er Anrufe von beliebig vielen Hinauswahlrechnern empfangen.

expect-send Ein Skriptformat, das in PPP- und UUCP-Chat-Skripten verwendet wird. Das Chat-Skript beginnt mit dem Text oder der Anweisung, die vom Remote-Peer *erwartet* wird. In der nächsten Zeile ist die Antwort enthalten, die vom lokalen Host *gesendet* werden soll, nachdem dieser die richtige expect-Zeichenfolge vom Peer erhalten hat. In den nachfolgenden Zeilen werden die expect-send-Anweisungen zwischen dem lokalen Host und dem Peer wiederholt, bis alle zum Kommunikationsaufbau benötigten Anweisungen erfolgreich ausgehandelt sind.

Extended Accounting Eine Funktion zum flexiblen Aufzeichnen des Ressourcenverbrauchs im Rahmen einer Aufgabe oder eines Prozesses.

Hinauswahlrechner Der Peer, der den Anruf initiiert, um eine PPP-Wählverbindung aufzubauen. Sobald der Hinauswahlrechner konfiguriert ist, kann es eine beliebige Anzahl von Einwahlservern anwählen. Der Hinauswahlrechner stellt normalerweise Authentifizierungs-Berechtigungsnachweise bereit, bevor eine Wählverbindung aufgebaut wird.

IPCP (Internet Protocol Control Protocol) Ein Unterprotokoll des PPP, das die IP-Adressen der Peers für die Verbindung aushandelt. IPCP handelt auch die Header-Komprimierung für die Verbindung aus und ermöglicht die Verwendung des Netzwerkebenenprotokolls.

IPV6CP (Internet Protocol Version 6 Control Protocol) Siehe IPCP (Internet Protocol Control Protocol).

ISDN-Terminal-Adapter (TA) Ein Gerät zur Anpassung von Signalen, das eine modemähnliche Schnittstelle für eine PPP-Einwahlverbindung über ein ISDN-Netzwerk bereitstellt. Verwenden Sie zum Konfigurieren eines ISDN-TA die Konfigurationsdateien von Solaris PPP 4.0 wie zum Konfigurieren eines Standardmodem.

LCP (Link Control Protocol) Ein Unterprotokoll des PPP, das verwendet wird, um die anfänglichen Parameter zwischen den Peers auszuhandeln. Zu den Funktionen des LCP gehört das Prüfen der Verbindungsintegrität. Aus diesem Grunde manifestieren sich viele verbindungsrelevante Probleme als LCP-Fehler.

MS-CHAP (Microsoft CHAP) Ein spezifisches Microsoft-Authentifizierungsprotokoll für PPP. Solaris PPP 4.0 unterstützt die Versionen 1 und 2 dieses Protokolls sowohl im Client- als auch im Servermodus.

Multicasting Eine Netzwerkschichtverfahren, das verwendet wird, um Datagrammpakete an mehreren Rechnern in einem IP-Netzwerk zu senden. Beim Broadcast-Routing werden Pakete nicht von jedem Rechner ausgehandelt. Multicast erfordert, dass Router mit speziellen Routing-Protokollen konfiguriert werden.

PAP (Password Authentication Protocol)

Ein Authentifizierungsprotokoll, das verwendet werden kann, um die Identität eines aufrufenden Programms über eine PPP-Verbindung zu verifizieren. Das PAP verwendet ein Klartextpasswort, das über die Verbindung weitergegeben wird, wodurch das Passwort auf einem der Endpunktrechner gespeichert werden kann. Ein PAP kann beispielsweise die Anmelde- und Passworteinträge der UNIX-Datenbank `passwd` verwenden, die sich auf dem Rechner befindet, der aufgefordert wird, die Identität des aufrufenden Programms zu verifizieren.

Siehe auch CHAP.

Peer

Ein einzelner Computer an einem Ende einer PPP-Kommunikationsverbindung, die aus zwei Peers besteht, die durch Kommunikationsmedien miteinander verbunden sind. Sie können viele Arten von Datenverarbeitungsgeräten als Peer konfigurieren, beispielsweise eine Workstation, einen PC, einen Router oder einen Großrechner.

PPP (Point-to-Point Protocol)

Ein Sicherungsschichtprotokoll, dass ein Standardverfahren für die Übertragung von Datagrammen über Point-to-Point-Medien bietet. Eine PPP-Konfiguration besteht aus zwei Endpunktsystemen, die als *Peers* bezeichnet werden, und den Telefonleitungen oder anderen bidirektionalen Verbindungen, die von Peers für die Kommunikation verwendet werden. Die Hardware- und Softwareverbindung zwischen den beiden Peers wird als *PPP-Verbindung* betrachtet.

PPP besteht aus einer Reihe von Unterprotokollen, darunter PAP, CHAP, LCP und CCP. Es stehen zahlreiche PPP-Implementierungen zur Verfügung.

PPP-Standleitungsverbindung

Eine PPP-Verbindung mit einem Host und einer CSU/DSU, die mit einem synchronen Netzwerkmedium über eine Standleitung verbunden sind. OC3 und T1 sind Beispiele für Standleitungsmedien. Standleitungsverbindungen sind zwar einfacher zu verwalten, aber sie sind auch teurer als PPP-Wählverbindungen und werden daher weniger häufig verwendet.

PPP-Wählverbindung

Eine PPP-Verbindung, die mit einem Peer und einem Modem an jedem Ende einer Telefonleitung oder ähnlichen ISDN-Kommunikationsgeräten aufgebaut wird. Der Begriff "Wählverbindung" bezieht sich auf den Vorgang der Aushandlung einer Verbindung, wenn ein lokales Modem einen Remote-Peer anwählt, indem es die Telefonnummer des Peers verwendet. Die Wählverbindung ist die gebräuchlichste und kostengünstigste PPP-Konfiguration.

PPPoE (PPP over Ethernet)

Ein spezifisches Protokoll von RedBack Networks, das Hosts ermöglicht, PPP-Sitzungen über eine Ethernet-Verbindung durchzuführen. PPPoE wird im Allgemeinen mit DSL-Services (Digital Subscriber Line) verwendet.

Service-Advertisements

Informationen zu einem Service, die von einem SA verteilt werden. Ein Service-Advertisement besteht aus einer URL und einer Reihe von Attribut-/Wertlistenpaaren, die einen Service beschreiben. Alle Service-Advertisements haben eine Lebensdauer. Nach Ablauf der Lebensdauer verliert ein Service-Advertisement seine Gültigkeit, es sei denn, es wird neu registriert.

Service-URL
Eine URL, die verwendet wird, um die Netzwerkadresse von Services bekannt zu geben. Die URL enthält den Servicetyp, den Hostnamen oder die Netzwerkadresse des Servicehosts. Die URL kann auch eine Portnummer und andere Informationen enthalten, die zur Verwendung dieses Service benötigt werden.

Serviceagent (Service Agent, SA)
Der SLP-Agent, der die Service-Advertisements für Netzwerkdienste verwaltet. Wenn kein DA (Directory Agent) verfügbar ist, beantwortet der SA die Multicast-Serviceanforderungen von UAs (User Agent). Wenn ein DA verfügbar ist, registriert der SA Services mit DAs bzw. hebt die Registrierung dieser auf, die seine Bereiche unterstützen.

SLPD (SLP daemon)
Der Dämonprozess, der als DA- oder SA-Server in der Oracle Solaris-Implementierung von SLP fungiert. Serviceprozesse auf dem Host registrieren Service-Advertisements mit `SLPD`, anstatt die Advertisements einzeln zu verwalten. Jeder Prozess enthält eine SA-Clientbibliothek, die mit `SLPD` kommuniziert, wenn der Dämon als SA-Server konfiguriert wird. Der SLP-Dämon leitet alle Registrierungen und Aufhebungen von Registrierungen an DAs weiter. Der Dämon löst eine Zeitbegrenzung für abgelaufene Service-Advertisements aus und verwaltet eine Tabelle von verfügbaren DAs, indem er eine aktive und passive DA-Ermittlung durchführt. Durch solche Mechanismen werden DA-Informationen für UA-Clients bereitgestellt. Auf UA-Clients wird `SLPD` auf einem Host nur zum Beziehen von DA-Informationen verwendet. Sie können `SLPD` optional als DA konfigurieren.

Synchrones PPP
Ein PPP, das über synchrone digitale Leitungen läuft, die Daten als kontinuierlichen Strom von Rohbits übertragen. Bei der PPP-Standleitungsverbindung wird ein synchrones PPP verwendet.

Veraltete Services
Ein Netzwerkdienst, das nicht SLP-fähig ist. Sie können eine Proxyregistrierung erstellen, um einen veralteten Service für SLP zu registrieren. SLP-basierte Clients können dann veraltete Services ermitteln (siehe Kapitel 10, „Integrieren von veralteten Services“).

Verbindung
Die Kommunikationsverbindung im PPP, die zwischen zwei Peers ausgehandelt und aufgebaut wird. Solaris PPP 4.0 unterstützt zwei Verbindungsarten: Einwahl- und Standleitungsverbindungen.

Vertrauenswürdige aufrufende Programme/Anrufer
Im Zusammenhang mit einem PPP handelt es sich hierbei um Remote-Peers, auf die ein Einwahlserver Zugriff gewährt, indem die Sicherheitsberechtigungsnachweise des Peers in die PAP- oder CHAP-Geheimnisdatenbank des Servers aufgenommen werden.

Verzeichnisagent (Directory Agent, DA)
Optionaler SLP-Agent, der einen Cache mit Service-Advertisements speichert und verwaltet, die vom Serviceagent (Service Agent, SA) gesendet werden. Sobald der DA bereitgestellt ist, löst er Serviceanforderungen des Benutzeragenten (User Agent, UA) auf. Der DA antwortet auf aktive Abrufe vom SA und vom UA für Verzeichnis-Advertisements. Infolge dessen ermitteln der SA und der UA die entsprechenden DAs und *Bereiche*. Ein DA sendet periodisch nicht angeforderte Advertisements, mit deren Hilfe UAs und SAs den DA innerhalb der gemeinsam genutzten Bereiche ermitteln.

Index

Zahlen und Symbole

- (Bindestrich)
  Feld "Line2", Platzhalter, 607
  in autofs Map-Namen, 228
  Platzhalter für das Feld "Speed", 600
  Wählcodekürzel, 601
= (Gleichheitszeichen), Wählcodekürzel, 601
(Nummernzeichen)
  Kommentare in der Master-Map (auto_master), 214
  Kommentare in direkten Maps, 216
  Kommentare in indirekten Maps, 217
+ (Pluszeichen)
  `/etc/hosts.equiv`-Dateisyntax, 681, 682
  in autofs-Map-Namen, 228, 229
. (Punkt)
  `rcp`-Befehlssyntax, 698, 700
/ (Schrägstrich)
  /- als Master-Map-Einhängepunkt, 213, 216
  Master-Map-Namen mit vorangestelltem, 213
  Root-Verzeichnis
    durch Clients ohne lokalen Massenspeicher einhängen, 77
* (Sternchen), in autofs-Maps, 233
~ (Tilde)
  abgekürzte Pfadnamen, 696, 697
  `rcp`-Befehlssyntax, 698, 700
\ (umgekehrter Schrägstrich) in Maps, 214, 216, 217
& (Und-Zeichen), in autofs-Maps, 232
(C.) UUCP-Arbeitsdateien (C.), Beschreibung, 633
!utomatische Freigabe von Dateisystemen, 86
(X.) UUCP-Dateien ausführen, uuxqt-Ausführung, 581

A

`-Ac`-Option, `sendmail`-Befehl, 403
`-Am`-Option, `sendmail`-Befehl, 403
`-a`-Option
  `showmount`-Befehl, 178
  `umount`-Befehl, 169
Abbrechen, Remote-Anmeldungen, 680
Abbruch des Einhängens durch Tastaturbefehl, 125
Abgeworfene Pakete, 705
Abmelden (Remote-Systeme), 688
Abweichungsdatei, 70
ACU (Automatic Call Unit)
  `Devices`-Datei, Feld "Type", 606
  UUCP-Hardwarekonfiguration, 579
Adresszuweisung
  PPP, 556, 557, 558
Aktivieren
  clientseitiges Failover, 94
  Echoprüfung, 614
  NCA, 53–55
  NCA-Protokollierung, 56
  NFS-Serverprotokollierung, 89–90
  Rückruf durch ein Chat-Skript aktivieren, 603
  Secure NFS-System, 102
  WebNFS-Service, 88
Aktueller Benutzer, 697
`aliasadm`-Befehl, 367

Aliase
Definition, 362
erstellen, 362
Erstellen, 363
/etc/mail/aliases-Datei, 380
NIS-Map aliases, 381
Schleifen, 344
verifizieren, 344
aliases, NIS+-Tabelle mail_aliases, 382
aliases-Datei, 368, 591
aliases.db-Datei, 332, 368
aliases.dir-Datei, 332, 368
aliases-NIS-Map, 381
aliases.pag-Datei, 332, 368
ALL-Wert in der COMMANDS-Option, 625
already mounted (Meldung), 132
Alternative Befehle, sendmail-Befehl, 354
Anbietereinstellung, Angeben in sendmail.cf Datei, 354
Ändern
/etc/shells-Datei, 342
.forward-Dateisuchpfad, 341
Anmelden
Entfernen von UUCP-Protokolldateien, 589
Remote-Anmeldungen
Authentifizierung (rlogin), 680, 683
direkt oder indirekt (rlogin), 683
direkte oder indirekt (rlogin), 683
feststellen, wer angemeldet ist, 686
ftp-Befehl, 690
FTP-Verbindung öffnen, 690, 691
FTP-Verbindung schließen, 691
mit rlogin, 680, 687, 688
sequentielle Anmeldungen, 683
unterbrechen, 680
Anmeldungen (UUCP)
Hinzufügen, 586, 587
Privilegien, 626
privilegiert, 625
anon-Option, share-Befehl, 173
anonyme FTP-Benutzer, Einrichten, 658
Anonymer FTP, Konten, 689
ANU (Australian National University) PPP, Kompatibilität mit Solaris PPP 4.0, 422
Anwendungen, hängend, 138
Any – Eintrag im Feld "Time", 598
Any-Schlüsselwort
Feld "Speed" (UUCP), 600
Any Schlüsselwort, Grades-Datei (UUCP), 630
Any-Schlüsselwort
Grades-Datei (UUCP), 631
Anzeigen von Netzwerkinformationen, 703, 704, 705, 711
Arbeitsverzeichnis, Definition des rcp-Befehls, 697
ARCH-Map-Variable, 227
asppp, *Siehe* Asynchronous PPP (asppp)
asppp2pppd-Konvertierungsskript
asppp-Standardkonfiguration, 571
Dateien anzeigen, die in Solaris PPP 4.0 konvertiert wurden, 575
in Solaris PPP 4.0 konvertieren, 575
ASSERT-Fehlermeldungen (UUCP), 594, 635, 636
Asynchrones PPP (asppp), UUCP-Datenbanken konfigurieren, 584
Asynchronous PPP (asppp)
Dateien in einer Konfiguration, 571
Dokumentation, 422
in Solaris PPP 4.0 konvertieren, 575
Unterschied zu Solaris PPP 4.0, 423
asyncmap-Option (PPP), 532
Audiodateien, Speicherplatzbedarf von Mailboxen und, 365
Aufheben der gemeinsamen Nutzung und erneutes Freigeben zur gemeinsamen Nutzung, NFS-Version 4, 188–189
Aufheben der gemeinsamen Nutzung von Dateisystemen, unshare-Befehl, 177
Auflisten
Clients mit Dateisystemen, die per Remote-Zugriff eingehängt wurden, 178
eingehängte Dateisysteme, 169
gemeinsam genutzte Dateisysteme, 175
Aufrufen von Remote-Computern (UUCP), 583
Aufrufen von Remote-Rechnern (UUCP), 628
Ausführbare Maps, 229
Ausführen von SMTP mit TLS
aufgabenbezogene Informationen, 317–322
Beschreibung, 392–397

Ausführen von SMTP mit TLS *(Fortsetzung)*
Konfigurationsdateioptionen für, 394–396
Makros für, 396
Regellisten für, 396–397
Sicherheitsüberlegungen zu, 397
Ausgeben
Liste von gemeinsam genutzten oder exportierten Dateien, 178
Liste von Verzeichnissen, die per Remote-Zugriff eingehängt wurden, 178
Aushandlung
Dateiübertragungsgröße, 200–201
WebNFS-Sicherheit, 83
Aushängen
autofs und, 77, 222
Beispiele, 169
Gruppen von Dateisystemen, 170
`auth`-Option (PPP), 482
Authentifizierer (PPP), 432
Authentifizierung
Siehe auch Authentifizierung (PPP)
allgemeine Probleme beheben, 523–524
DH, 210, 211
Remote-Anmeldungen mit `ftp`-Befehl, 689, 690, 691
Remote-Anmeldungen mit `rlogin`-Befehl, 680, 683, 687
direkte oder indirekte Anmeldungen, 683
`/etc/hosts.equiv`-Datei, 681, 682
Netzwerkauthentifizierung oder Remote-Systemauthentifizierung, 680, 682, 683
`.rhosts`-Dateien, 682, 683
RPC, 210
UNIX, 208, 210
Authentifizierung (PPP)
Authentifizierer, 432
Authentifizierungsempfänger, 432
Beispiel für CHAP, 448
Beispiel für PAP, 446
CHAP-Berechtigungsnachweise konfigurieren, 491
CHAP konfigurieren
Siehe auch CHAP (Challenge-Handshake Authentication Protocol)
Authentifizierung (PPP), CHAP konfigurieren *(Fortsetzung)*
Einwahlserver, 488, 490
Hinauswahlrechner, 492–493
Datenbank für CHAP-Berechtigungsnachweise konfigurieren, 488–489
Geheimnisdatei
für PPP, 432
PAP konfigurieren
Siehe auch PAP (Password Authentication Protocol)
planen, 445, 448
Prozessdiagramm
für PAP, 550
secrets-Datei
für PAP, 481
Standardrichtlinie, 431
Übersicht der Schritte zum Konfigurieren, 478–479, 487–488
Übersichten der Schritte zum Konfigurieren, 477–478
Unterstützung für Standleitungen, 432
vertrauenswürdiges aufrufendes Programm, 432
Voraussetzungen vor dem Konfigurieren, 445
Authentifizierungsempfänger (PPP), 432
authentische FTP-Benutzer, Einrichten, 656
`auto_direct`-Datei, 307
`auto_home`-Map
`/home` Einhängepunkt, 213
`/home`-Einhängepunkt, 214
`/home`-Verzeichnis, 116
`/home`-Verzeichnisserver einrichten, 116
`auto_master`-map, 104
autofs
Aushängeprozess, 222
Betriebssysteme
kompatible Versionen unterstützen, 120
Dateisysteme einhängen, 92
Durchsuchfunktion, 84, 122
Einhängeprozess, 221, 222
Fehlerbehebung, 131
Funktionen, 84
gemeinsam genutzte Dateien auf mehreren Servern replizieren, 121

autofs *(Fortsetzung)*
/home-Verzeichnis, 116
Home-Verzeichnisserver einrichten, 116
Maps
Arten, 110
Auswahl schreibgeschützter Dateien, 223, 226
Bezugnahme auf andere Maps, 228, 229
cachefs-Option, 115
CD-ROM-Dateisystem, 114
direkte, 215, 216
Durchsuchfunktion und, 84
hsfs-Option, 114
indirekte, 217, 218
Master, 213
Navigationsprozess starten, 221
Navigationsprozesse starten, 214
Netzwerknavigation, 220
PC-DOS-Dateisystem, 114
pcfs-Option, 114
Variablen, 227
Maps verwalten, 110
Metazeichen, 232, 233
Namespace-Daten, 84
NFS-URL und, 122
projektbezogene Dateien konsolidieren, 117
Referenz, 232, 233
Routine für den Zugriff auf öffentliche Dateien und, 122
Sonderzeichen, 233
starten, 98
stoppen, 98
Übersicht, 77
Zugriff auf ein Nicht-NFS-Dateisystem, 114
Zugriff auf einen gemeinsam genutzten Namespace, 119
Zugriff auf Nicht-NFS-Dateisysteme, 113
Automatic Call Unit (ACU), Fehlerbehebung, 592
Automatische Freigabe von Dateisystemen, 86
Automatisches Einhängen
/var/mail-Verzeichnis, 307, 364
automount-Befehl, 161
autofs-Map modifizieren (auto_master), 111
autofs und, 77
Fehlermeldungen, 131
automount-Befehl *(Fortsetzung)*
Übersicht, 219
-v-Option, 131
Zeitpunkt der Ausführung, 111
automountd-Dämon, 147–148
autofs und, 77
Beschreibung, 84
Einhängen und, 84
Übersicht, 219

B

b (Escape-Zeichen), Dialers-Datei, 614
-bP-Option, sendmail-Befehl, 404
bad argument with index option, 135
bad key (Meldung), 131
Befehle
(X.) UUCP-Dateien ausführen, 581
hängende Programme, 138
Remote-Ausführung mit UUCP, 620, 623, 626
UUCP-Ausführungsdateien (X.), 634
UUCP Fehlerbehebung, 595
Befehlszeilenoptionen ab Version 8.12
sendmail-Befehl, 402, 403, 404
Beispiel, PPP-Konfigurationen, *Siehe*
Konfigurationsbeispiele für PPP
Benutzeragent (SLP), 253
Benutzernamen
aktueller Benutzer, 697
direkte oder indirekte Anmeldungen (rlogin), 683
feststellen, welche Benutzer beim Remote-System angemeldet sind, 686
nach Benutzern suchen, die bei Remote-System angemeldet sind, 686
Benutzernamen, Mailbox-Namen und, 361
Berechtigungen
Anforderungen für das Kopieren, 698
vbsr der NFS-Version 3, 78
Berechtigungsnachweise
Beschreibung, 209
CHAP-Authentifizierung, 488–489
PAP-Authentifizierung, 480–481
UNIX-Authentifizierung, 210

Bereiche (SLP)
bereitstellen, 267–270
DAs und, 255, 271
default-Bereich, 268
Definition, 237
Multihomed-Hosts und, 278
Proxytegistrierung und, 282
Überlegungen, 268–269
wann eine Konfiguration erforderlich ist, 268
Betriebssysteme
Map-Variablen, 227
nicht kompatible Versionen unterstützen, 120
bg-Option, mount-Befehl, 163
Bindestrich (-)
Feld "Line2", Platzhalter, 607
in autofs-Map-Namen, 228
Platzhalter für das Feld "Speed", 600
Wählcodekürzel, 601
Boot-Vorgang, Dateisysteme einhängen, 91
Booten, Sicherheit von Clients ohne lokalen Massenspeicher, 212
Break-Escape-Zeichen, Dialers-Datei, 614
Broadcast (SLP), 261, 271, 275
bye-Befehl (FTP), 691

C

c (Escape-Zeichen), Dialers-Datei, 614
Cache-Dateisystem
autofs-Zugriff mit, 114, 115
Cache und NFS-Version 3, 78
cachefs-Option, autofs-Maps, 115
call-Option (PPP), einen Einwahlserver aufrufen, 470
Callback
Permissions-Dateioption, 623
Rückruf durch ein Chat-Skript aktivieren, 603
CALLBACK-Option der Permissions-Datei, 623
can't mount (Meldung), 132
cannot receive reply (Meldung), 134
cannot send packet (Meldung), 134
cannot use index option without public option (Meldung), 135
CD-ROM-Anwendungen, mit autofs zugreifen, 113
cfsadmin-Befehl, auf NFS-Dateisysteme zugreifen, 115
CHAP (Challenge-Handshake Authentication Protocol)
Authentifizierungsprozess, 556
Beispielkonfiguration, 448
Definition, 552
Syntax der /etc/ppp/chap-secrets, 553
Übersicht der Schritte zum Konfigurieren, 487–488
chat-Programm in PPP, *Siehe* Chat-Skript
Chat-Skript
Aufrufen, in PPP, 547–548
Beispiele (PPP)
Chat-Skript für die UNIX-basierte Anmeldung, 543–545
für einen ISDN-TA, 545–546, 546
grundlegendes Modem-Chat-Skript, 539–541
Skript zum Aufrufen eines ISP, 542–543
UNIX-basiertes Anmelde-Chat-Skript, 461
Chat-Skript erstellen, 538
ein ausführbares Chat-Programm erstellen, 548
Chat-Skript für einen Terminal-Adapter (TA), 545–546, 546
check_eoh-Regelliste, sendmail-Befehl, 416
check_etrn-Regelliste, sendmail-Befehl, 417
check_expn-Regelliste, sendmail-Befehl, 417
check-hostname-Skript, 309, 311, 373
check-permissions-Skript, 373
check_vrfy-Regelliste, sendmail-Befehl, 417
chkey-Befehl, Secure NFS aktivieren, 102
clear_locks-Befehl, 161–162
clientmqueue-Verzeichnis, 373
Clients
Siehe auch Mailclients, NFS-Clients, NTP-Client und PPPoE-Client
Aufrufe von Servern verfolgen, 703, 705
Informationen anzeigen über, 703, 709, 711
Clients ohne lokalen Massenspeicher
Anforderungen für das manuelle Einhängen, 77
Sicherheit während des Boot-Vorgangs, 212
Clientseitiges Failover
aktivieren, 94
in NFS-Version 4, 204
NFS-Sperrung und, 204

Clientseitiges Failover *(Fortsetzung)*
NFS-Unterstützung, 81
replizierte Dateisysteme, 203–204
Terminologie, 203
clientseitiges Failover, Übersicht, 202–204
Clientwiederherstellung, NFS-Version 4, 192–194
COMMANDS-Option der
`Permissions`-Datei, 623–625, 627
VALIDATE-Option, 626
`compat_check FEATURE()`-Deklaration, 409
`confFORWARD_PATH` Definition, 341
`confFORWARD_PATH`-Definition, 341
`connect`-Option (PPP)
Beispiel, 463
um ein Chat-Skript aufzurufen, 546
could not use public filehandle (Meldung), 136
couldn't create mount point (Meldung), 132
CPU-Map-Variable, 227
`crontab`-Datei, für UUCP, 587
`crtscts`-Option (PPP), 460
CSU/DSU
allgemeine Probleme beheben, 523
Definition, 430
konfigurieren, 473
`cu`-Befehl
Beschreibung, 582
mehrere oder verschiedene
Konfigurationsdateien, 583, 617
`Systems`-Listen ausgeben, 618
`cu` Befehl, Überprüfen von Modems oder ACUs, 592

D

`D.` UUCP-Datendateien, Entfernen, 589
`D`-Escape-Zeichen, 610
`d`-Escape-Zeichen, `Dialers`-Datei, 614
`-d` Option, `cu` Befehl, 592
`-d`-Option, `showmount`-Befehl, 178
DA_BUSY_NOW, 273
DA-Erkennung (SLP), 263
DA-Takt, Häufigkeit, 252
daemon running already (Meldung), 136
Dämonen
`automountd`, 147–148
Dämonen, `automountd` *(Fortsetzung)*
autofs und, 77
Übersicht, 219
erforderlich für das Remote-Einhängen, 124
`lockd`, 148–149
`mountd`, 149
Antwort des Servers prüfen, 127
Betrieb prüfen, 129, 137
nicht registriert mit `rpcbind`, 137
`nfs4cbd`, 149
`nfsd`
Antwort des Servers prüfen, 127
Beschreibung, 150
Betrieb prüfen, 129
`nfslogd`, 150–151
`nfsmapid`, 151–159
`rpcbind`
mount (Fehlermeldungen), 137
`statd`, 159–160
DAs (SLP)
Advertisement, 252, 254, 255, 256
aktive Erkennung deaktivieren, 254
bereitstellen, 257, 270–271
DA-Protokollierung, 271
DFÜ-Netzwerke erkennen, 256
entfernen, 256
Erkennung, 252, 257, 268
Erkennung von DFÜ-Netzwerken, 254
Ermittlung von Einwahlnetzwerken, 663
mehrere DAs, 273–274
Multicast, 257
Multicast beenden, 254
ohne Multicast, 275
passive Erkennung deaktivieren, 253
Takt, 255–256, 256, 258
Dateiattribute und NFS-Version 3, 78
Dateiberechtigungen
Verbesserung der NFS-Version 3, 78
WebNFS und, 106
Dateien und Dateisysteme
abgekürzte Pfadnamen, 696, 697
Auswahl von Dateien durch autofs, 223, 226
autofs-Zugriff
NFS-Dateisysteme mit CacheFS, 114, 115

Dateien und Dateisysteme, autofs-Zugriff *(Fortsetzung)*
Nicht-NFS-Dateisysteme, 113, 114
automatische Freigabe, 86
definierte Dateisysteme, 75
lokale Dateisysteme
Gruppen aushängen, 170
NFS-ASCII-Dateien und ihre Funktionen, 142
NFS-Behandlung von, 75
NFS-Dateien und ihre Funktionen, 141
projektbezogene Dateien konsolidieren, 117
Remote-Dateisysteme
aus der Dateisystemtabelle einhängen, 170
Clients mit Dateisystemen auflisten, die per Remote-Zugriff eingehängt wurden, 178
Gruppen aushängen, 170
Dateisystem-Namespace, NFS-Version 4, 189–191
Dateisysteme
Netzwerkstatistiken für, 709, 711
Dateisysteme und NFS, 75
Dateiübertragungen (UUCP)
Arbeitsdateien (C.), 633, 634
Berechtigungen, 620, 623
Dämon, 580
Fehlerbehebung, 594
Fehlersuche, 592
Dateiübertragungsgröße, Aushandlung, 200–201
Datenbank für CHAP-Berechtigungsnachweise
erstellen
für einen Einwahlserver, 488–489
Erstellen
für vertrauenswürdige Anrufer, 491
Datenbank für PAP-Berechtigungsnachweise
erstellen
für einen Einwahlserver, 480
für vertrauenswürdige Anrufer, 483–484
für einen Einwahlserver erstellen, 480–481
Datum, mit einem anderen System synchronisieren, 69
deaktivieren
autofs-Durchsuchfunktion
Aufgaben, 122
Überblick, 122
Deaktivieren
Echoprüfung, 614
Einhängezugriff eines Clients, 94–95
Deaktivieren *(Fortsetzung)*
Erstellung großer Dateien, 93
`.forward`-Dateien, 340
NCA, 56
NCA-Protokollierung, 56
`delay_checks` `FEATURE()`-Deklaration, 409
Delegierung, NFS-Version 4, 195–197
Delivery Agent-Flags ab Version 8.12, `sendmail` Befehl, 412
`demand`-Initialisierungsskript für PPP, 475
Desktop-Publishing-Dateien, Speicherplatzbedarf für Mailboxen und, 365
`/dev/nca`-Datei, NCA und, 63
`Devconfig`-Datei
Beschreibung, 583, 631
Format, 631
`Devices`-Datei
Beschreibung, 583, 605
Feld "Class", 607
Feld "Dialer-Token-Pairs", 608, 610
Feld "Line", 607
Feld "Line2", 607
Feld "Type", 606
Format, 605
mehrere oder verschiedene Dateien, 617
Protokolldefinitionen, 611
`Systems`-Datei, Feld "Speed" und, 600
`Systems`-Datei, Feld "Typ" und, 606
`dfstab`-Datei
automatische gemeinsame Nutzung von Dateisystemen, 87
Einhängezugriff eines Clients deaktivieren, 94
NFS-Serverprotokollierung aktivieren, 89
Secure NFS aktivieren, 103
Secure NFS-Option, 103
Syntax für NFS-Dateisysteme, 87
WebNFS-Service aktivieren, 88
DH-Authentifizierung
Benutzerauthentifizierung, 208
`dfstab`-Dateioption, 103
Passwortschutz, 209
Secure NFS und, 102
Übersicht, 210, 211

Diagnose für PPP
  aktivieren
    mit pppd,, 507–508
  -Fehlersuche Option, 508
  Protokolldatei für einen PPPoE-Tunnel, 521
  Standleitungsverbindung, 507
  Wählverbindung, 507
Dialcodes-Datei, 583, 616
Dialers-Datei
  Beispiel, 613
  Beschreibung, 583, 612
Dialogschlüssel, 211
dir must start with '/' (Meldung), 133
direct-Schlüsselwort des Felds "DTP", 608
Direct-Schlüsselwort des Felds "Type", 606
Direkte E/A-Einhängung (Option), 163
direkte Maps (autofs), Beispiel, 215
Direkte Maps (autofs)
  Beschreibung, 110
  Kommentare in, 216
  modifizieren, 112
  Syntax, 215
  Übersicht, 216
  wann das Ausführen erforderlich
    istautomount-Befehl, 111
Direkte Remote-Anmeldungen
  indirekte Anmeldungen oder
    rlogin-Befehl, 683
direkte Remote-Anmeldungen
  indirekte Anmeldungen oder
    rlogin-Befehl, 683
Direkte Remote-Anmeldungen
  mit rlogin-Befehl, 687, 688
Direkte Verbindung, UUCP-Konfiguration, 579
dnsbl FEATURE()-Deklaration, 409, 411
domain-Verzeichnis, 371
Domainnamen, Secure NFS-System und, 102
Domains
  Definition, 102
  Remote-Anmeldungen und, 680
  Teildomains und, 358
DOS-Dateien, mit autofs zugreifen, 114
dot (.)
  in Domainadressen, 360
dot (.) *(Fortsetzung)*
  in Mailbox-Namen, 361
DSL, *Siehe* PPPoE
DSL-Modem, 436
DSLAM (Digital Subscriber Line Access Multiplexer)
  für PPPoE, 436
dtmail-Mail-Benutzeragent, 373
Durchsuchfunktion
  deaktivieren, 122
  Übersicht, 84
Dynamische Adressierung, PPP, 556

E

E-Escape-Zeichen, Dialers-Datei, 614
e-Escape-Zeichen, Dialers-Datei, 614
E-Mail, UUCP-Verwaltung, 591
e-Protokoll in Devices-Datei, 611
-e-Option, showmount-Befehl, 178
Echoprüfung, 614
editmap-Befehl, 373
eingehende Kommunikation, Callback-Sicherheit, 623
Eingehende Kommunikation
  Callback-Sicherheit, 623
  durch ein UUCP-Chat-Skript aktivieren, 603
Einhängen
  Abbruch durch Tastaturbefehl während, 125
  alle Dateisysteme in einer Tabelle, 170
  Anforderungen für Clients ohne lokalen
    Massenspeicher, 77
  autofs und, 77, 222
  Beispiele, 167
  bereits eingehängtes Dateisystem überlagern, 167
  erneute Versuche im Hintergrund, 163
  erneute Versuche im Vordergrund, 163
  Lese- und Schreibzugriff, 166
  nfsd-Dämon und, 201–202
  Portmapper und, 201–202
  Remote-Einhängen
    erforderliche Dämonen, 124
    Fehlerbehebung, 126–127, 129
  Routine für den Zugriff auf öffentliche Dateien
    und, 201
  schreibgeschützt, 166, 167

Einhängen *(Fortsetzung)*
/var/mail-Verzeichnis, 307
weiches Einhängen im Vergleich mit hartem Einhängen, 125
Einhängen von Dateien im Hintergrund (Option), 163
Einhängen von Dateien im Vordergrund (Option), 163
Einhängen von Dateisystemen
autofs und, 92
manuell (ohne Vorbereitung), 92
NFS-URL mit, 95–96
über eine Firewall, 95
Übersicht, 90
Übersicht der Schritte, 90
während des Boot-Vorgangs einhängen, 91
Zugriff eines Clients deaktivieren, 94–95
Einhängepunkte
/- als Master-Map-Einhängepunkt, 213, 216
/home, 213, 214
Konflikte vermeiden, 112
/net, 214
Einrichten
lokale Mailaliasdatei, 331
mail.aliases-NIS-Map, 330
Mailclient, 307
Mailgateway, 310
Mailhost, 309
Mailserver, 339
virtueller Host, 315
Einrichten von SMTP zur Verwendung von TLS, 317–322
Eintrag im Feld "Never Time", 621
Einwahlserver
Aufrufe empfangen, 469–470
Definition, 426
konfigurieren
CHAP-Authentifizierung, 488, 490
Kommunikation über eine serielle Verbindung, 468–469, 532
Modem, 464–465
PAP-Authentifizierung, 480–481, 481–483
serieller Port, 464–465
Konten für PPP-Benutzer erstellen, 466
Planungsinformationen, 439, 466
Einwahlserver *(Fortsetzung)*
Übersicht der Schritte zum Konfigurieren, 464
UUCP, 603
Einwahlverbindung
Aufruf eines Peers initiieren, 469–470
Beispiel, 440
Chat-Skripten
UNIX-basierte Anmeldung, 543–545
Vorlage, 541–542
planen, 440
Übersicht der Schritte, 455
Vorlagen für Konfigurationsdateien, 457
Einzelbenutzermodus und Sicherheit, 211
enhdnsbl FEATURE()-Deklaration, 409, 411
Entfernen von Sperren, 161–162
error checking (Meldung), 136
error locking (Meldung), 136
errors Verzeichnis (UUCP), 594
Erstellen
/etc/shells-Datei, 342
postmaster-Alias, 333
postmaster-Mailbox, 334
verschlüsselte Zuordnungsdatei, 333
Escape-Zeichen
Dialers-Datei, Sendezeichenfolgen, 613
Systems-Datei, Chat-Skript, 602
/etc/asppp.cf-Konfigurationsdatei, 572
/etc/auto_direct-Datei, 307
/etc/default/autofs-Datei, 143
autofs-Umgebung konfigurieren, 109
/etc/default/nfs-Datei, 79
/etc/default/nfs-Datei, Schlüsselwörter für, 144
/etc/default/nfslogd-Datei, 144–145
/etc/default/sendmail-Datei, 384
/etc/dfs/dfstab-Datei
automatische gemeinsame Nutzung von Dateisystemen, 87
Einhängezugriff eines Clients deaktivieren, 94
NFS-Serverprotokollierung aktivieren, 89
Secure NFS aktivieren, 103
Secure NFS-Option, 103
WebNFS-Service aktivieren, 88
/etc/hostname.*interface*-Datei, NCA und, 63
/etc/hosts-Datei, 63, 302, 303

/etc/hosts.equiv-Datei, 681, 682
/etc/inet/ntp.client-Datei, 70
/etc/inet/ntp.conf-Datei, 70
/etc/inet/ntp.keys-Datei, 70
/etc/inet/ntp.server-Datei, 70
/etc/inet/services-Datei, UUCP-Überprüfung, 590
/etc/inet/slp.conf-Datei
  Ändern der Konfiguration, 251
  DA-Advertisements, 254
  DA-Takt, 256
  DAs bereitstellen, 272
  Elemente, 250
  Lastausgleich, 274
  mit statischen DAs, 253
  Multicast-Lebensdauer, 259
  neue Bereiche, 267, 269
  Nur-Broadcast-Routing, 262
  Paketgröße, 261
  Proxyregistrierung, 283
  SA-Neuregistrierungen, 258
  Schnittstellen ändern, 277
  Übersicht, 243
  Zeitüberschreitungen, 264
  Zufallswartezeit, 266
/etc/init.d/ncakmod-Skript, 63
/etc/init.d/ncalogd-Skript, 63
/etc/init.d/slpd-Skript, 283
/etc/mail/aliases-Datei, 361, 368, 380
  UUCP und, 591
/etc/mail/aliases.db-Datei, 332, 368
/etc/mail/aliases.dir-Datei, 332, 368
/etc/mail/aliases.pag-Datei, 332, 368
/etc/mail/cf/cf/main.cf-Datei, 370
/etc/mail/cf/cf/main.mc-Datei, 370
/etc/mail/cf/cf/Makefile-Datei, 370
/etc/mail/cf/cf/sendmail.mc-Datei, 370
/etc/mail/cf/cf/submit.cf-Datei, 370
/etc/mail/cf/cf/submit.mc-Datei, 370
/etc/mail/cf/cf/subsidiary.cf-Datei, 370
/etc/mail/cf/cf/subsidiary.mc-Datei, 371
/etc/mail/cf/domain/generic.m4-Datei, 371
/etc/mail/cf/domain/solaris-antispam.m4-Datei, 371
/etc/mail/cf/domain/solaris-generic.m4-Datei, 371
/etc/mail/cf/domain-Verzeichnis, 371
/etc/mail/cf/feature-Verzeichnis, 371
/etc/mail/cf/m4-Verzeichnis, 371
/etc/mail/cf/mailer-Verzeichnis, 371
/etc/mail/cf/main-v7sun.mc-Datei, 371
/etc/mail/cf/ostype/solaris2.m4-Datei, 371
/etc/mail/cf/ostype/solaris2.ml.m4-Datei, 371
/etc/mail/cf/ostype/solaris2.pre5.m4-Datei, 371
/etc/mail/cf/ostype/solaris8.m4-Datei, 372
/etc/mail/cf/ostype-Verzeichnis, 371
/etc/mail/cf/README-Datei, 370
/etc/mail/cf/sh/check-hostname-Skript, 373
/etc/mail/cf/sh/check-permissions-Skript, 373
/etc/mail/cf/subsidiary-v7sun.mc-Datei, 372
/etc/mail/cf-Verzeichnis, Inhalt, 369
/etc/mail/helpfile-Datei, 369, 418
/etc/mail/local-host-names-Datei, 369, 418
/etc/mail/Mail.rc-Datei, 368
/etc/mail/mailx.rc-Datei, 368
/etc/mail/main.cf-Datei, 369
/etc/mail/relay-domains-Datei, 369
/etc/mail/sendmail.cf-Datei, 369
/etc/mail/sendmail.ct-Datei, 418
/etc/mail/sendmail.cw-Datei, 418
/etc/mail/sendmail.hf-Datei, 418
/etc/mail/sendmail.pid-Datei, 369
/etc/mail/statistics-Datei, 369
/etc/mail/submit.cf-Datei, 369, 401
/etc/mail/subsidiary.cf-Datei, 302, 369
/etc/mail/trusted-users-Datei, 369, 418
/etc/mail-Verzeichnis, Inhalt, 368
/etc/mnttab-Datei
  erstellen, 179
  mit der auto_master-Map vergleichen, 219
/etc/nca/nca.if-Datei, 63
/etc/nca/ncakmod.conf-Datei, 63
/etc/nca/ncalogd.conf-Datei, 63
/etc/nca/ncaport.conf-Datei, 63
/etc/netconfig-Datei, Beschreibung, 142
/etc/nfs/nfslog.conf-Datei, 145–147
  NFS-Serverprotokollierung aktivieren, 89
/etc/nsswitch.conf-Datei, 312, 681
/etc/passwd-Datei
  Aktivieren von UUCP-Anmeldungen, 586
  ftp und, 689

/etc/ppp/chap-secrets-Datei
  Adressierung
    durch sppp-Einheitennummer, 558
    statisch, 557
  Beispiel, für einen PPPoE-Zugangsserver, 566
  Definition, 526
  erstellen
    für vertrauenswürdige Anrufer, 491
  syntax, 553
/etc/ppp/myisp-chat.tmpl-Vorlage, 541–542
/etc/ppp/options-Datei
  Berechtigungen, 528
  Definition, 526, 530
  erstellen
    für einen Einwahlserver, 468
    für einen Hinauswahlrechner, 460
  /etc/ppp/options.tmpl-Vorlage, 530
/etc/ppp/options Datei, für die
  PAP-Authentifizierung modifizieren, 485
/etc/ppp/options-Datei
  Liste von Beispielen, 531
  name-Option für die CHAP-Authentifizierung, 490
  PPPoE-Beispiel, 566
/etc/ppp/options.tmpl-Vorlage, 530
/etc/ppp/options.ttya.tmpl-Vorlage, 533
/etc/ppp/options.*ttyname*-Datei
  Berechtigungen, 528
  Definition, 526, 531
  dynamische Adressierung, 556
  für einen Einwahlserver, 468, 532
  für einen Hinauswahlrechner, 460, 532
  Liste von Beispielen, 533
/etc/ppp/pap-secrets Datei
  Adressierung
    durch sppp-Einheitennummer, 558
/etc/ppp/pap-secrets-Datei
  Adressierung
    statisch, 557
  Beispiel, für einen PPPoE-Zugangsserver, 566
  Definition, 526
  erstellen
    für einen Einwahlserver, 481
    für einen PPPoE-Zugangsserver, 502
  für vertrauenswürdige Anrufer erstellen, 484
/etc/ppp/pap-secrets-Datei *(Fortsetzung)*
  Syntax, 549
/etc/ppp/peers/myisp.tmpl-Vorlage, 536
/etc/ppp/peers/*peer-name*-Datei
  Beispiel, für einen PPPoE-Client, 568
  Berechtigungen, 528
  Definition, 526, 535–536
  erstellen
    für ein Endpunkt an einer
      Standleitungsverbindung, 474
  Liste von Beispielen, 537
  modifizieren
    für die PAP-Authentifizierung, 486
    für einen PPPoE Client, 498
  nützliche Optionen, 535
/etc/ppp/peers-Verzeichnis, 526
/etc/ppp/pppoe-Datei
  Beispiel, 563, 565
  modifizieren, 501
  Services auflisten, 500
  Syntax, 562
/etc/ppp/pppoe.*device*-Datei
  Definition, 564
  für einen Zugangsserver, 502
  Syntax, 564
/etc/ppp/pppoe.if-Datei
  Beispiel, 560
  Definition, 559
  erstellen
    auf einem PPPoE-Client, 497
    für einen Zugangsserver, 500
/etc/.rootkey-Datei
  Secure NFS aktivieren, 103, 104
/etc/services-Datei, nfsd-Einträge, 135
/etc/shells-Datei, 342
/etc syslog.conf-Datei, 346
/etc/uucp/Config-Datei
  Beschreibung, 583, 628
  Format, 628
/etc/uucp/Devconfig-Datei
  Beschreibung, 583, 631
  Format, 631
/etc/uucp/Devices-Datei
  Beispiel für eine asppp-Konfiguration, 573

/etc/uucp/Devices-Datei *(Fortsetzung)*
Beschreibung, 583, 605
Feld "Class", 607
Feld "Dialer-Token-Pairs", 608, 610
Feld "Line", 607
Feld "Line2", 607
Feld "Type", 606
Format, 605
Protokolldefinitionen, 611
Systems-Datei, Feld "Speed" und, 600
Systems-Datei, Feld "Type" und, 606
/etc/uucp/Dialcodes-Datei, 583, 616
/etc/uucp/Dialers-Datei
Beispiel, 613
Beispiel für asppp-Konfiguration, 573
Beschreibung, 583, 612
/etc/uucp/Grades-Datei
Beschreibung, 583, 628
Feld "ID-list", 630, 631
Feld "Job-size", 630
Feld "Permit-type", 630
Feld "System-job-grade", 629, 630
Feld "User-job-grade", 629
Schlüsselwörter, 630
Standardklasse, 630
/etc/uucp/Limits-Datei
Beschreibung, 583, 632
Format, 632
/etc/uucp/Permissions-Datei
Ändern eines Knotennamens, 621
Beschreibung, 583, 619
CALLBACK-Option, 623
COMMANDS-Option, 623, 625, 627
Dateiübertragungsberechtigungen, 620, 623
Einrichten der Sicherheit, 590
Format, 619
LOGNAME
Anmelde-IDs für Remote-Computer, 620
Beschreibung, 619
Kombinieren mit MACHINE, 627
MACHINE
Beschreibung, 620
Kombinieren mit LOGNAME, 627
OTHER-Option, 626
/etc/uucp/Permissions-Datei, MACHINE *(Fortsetzung)*
standardmäßige Berechtigungen oder Beschränkungen, 620
MYNAME-Option, 621
NOREAD-Option, 622
NOWRITE-Option, 622
OTHER-Option, 626
READ-Option, 622
Remote-Ausführungsberechtigungen, 623, 626
REQUEST-Option, 620
Rückrufberechtigungen, 623
SENDFILES-Option, 620
Strukturierungseinträge, 619
Überlegungen, 620
uucheck-Befehl und, 582
uuxqt-Dämon und, 581
VALIDATE-Option, 625, 626
Weiterleitung, 627
WRITE-Option, 622
/etc/uucp/Poll-Datei
Beschreibung, 583, 628
Format, 628
/etc/uucp/Sysfiles-Datei
Beispiele, 618
Beschreibung, 583, 617
Format, 618
Systems-Liste ausgeben, 618
/etc/uucp/Sysname-Datei, 583, 618
/etc/uucp/Systems-Datei
Beispiel für eine asppp-Konfiguration, 572
Beschreibung, 583, 597
Devices-Datei, Feld "Class" und, 607
Devices-Datei, Feld "Type" und, 606
Escape-Zeichen, 602
Fehlerbehebung, 594
Feld "Chat Script", 601, 604
Feld "Phone", 601
Feld "Speed", 600
Feld "System-Name", 598
Feld "Time"
Beschreibung, 599
Never Eintrag, 621
Feld "Type", 600

/etc/uucp/Systems-Datei *(Fortsetzung)*
Format, 598
Hardware-Flusskonrolle, 604
Hardware-Flusskontrolle, 604
mehrere oder verschiedene Dateien, 583, 597, 617
Parität einstellen, 604
TCP/IP-Konfiguration, 589, 590
Wählcodekürzel, 583
/etc/vfstab-Datei
automount-Befehl und, 219
clientseitigen Failover aktivieren, 94
Dateisysteme während des Boot-Vorgangs einhängen, 91
durch Clients ohne lokalen Massenspeicher einhängen, 77
NFS-Server und, 91
nolargefiles-Option, 93
Ethernet, Mailkonfiguration prüfen, 343
etrn-Skript, 373
exit-Befehl, 688

F

f-Protokoll in Devices-Datei, 611
-F-Option, unshareall-Befehl, 178
Failover
Fehlermeldung, 136
mount-Befehl (Beispiel), 167
NFS-Unterstützung, 81
FEATURE()-Deklarationen in Version 8.12
nicht unterstützt, 411
unterstützt, 408
FEATURE()-Deklarationen in Version 8.13 von sendmail, 399–400
feature-Verzeichnis, 371
Fehler beim Öffnen, NFS und, 78
Fehlerbehebung
autofs, 131
Einhängepunktkonflikte vermeiden, 112
Fehlermeldungen, die von automount -v generiert werden, 131
verschiedene Fehlermeldungen, 133
Mailaliase, 344
MAILER-DAEMON-Meldungen und, 347
Fehlerbehebung *(Fortsetzung)*
Mailservices, 342
Mailverbindungen mit anderen Systemen, 346
Netzwerke, 709, 711
NFS
feststellen, an welchem Punkt der NFS-Service ausgefallen ist, 129
hängende Programme, 138
Remote-Einhängeprobleme, 125
Remote-Einhängungsprobleme, 137
Serverprobleme, 126
Strategien, 124
nicht übermittelte Mail, 344
Regellisten, 345
UUCP, 592, 638
ASSERT-Fehlermeldungen, 594, 635, 636
Befehle für die Fehlerbehebung, 595
fehlerhaftes Modem oder ACU, 592
Prüfen der Systems-Datei, 594
Prüfen von Fehlermeldungen, 594
Prüfen von grundlegenden Informationen, 595
STATUS-Fehlermeldungen, 594, 636, 638
Suche nach Übertragungsfehlern, 592, 594
Überprüfen von Fehlermeldungen, 638
Fehlermeldungen
Fehler beim Öffnen
NFS und, 78
generiert von automount -v, 131
No such file or directory, 137
Permission denied, 137
Schreibfehler
NFS und, 78
sendmail-Programm, 348
Server antwortet nicht
Abbruch durch Tastaturbefehl, 125
hängende Programme, 138
Remote-Einhängungsprobleme, 137, 138
verschiedene automount-Meldungen, 133
-Fehlersuche Option für PPP, 508
Fehlersuche
UUCP-Übertragungen, 592, 594
Fehlgeschlagene ID-Zuordnung, Gründe, 198
Feld "Chat Script", /etc/uucp/Systems-Datei, 601
Feld "Class", Devices-Datei, 607

Feld "Dialer-Token-Pairs"
Devices-Datei
Dialertypen, 608
gleicher Portselektor, 610
Syntax, 608
Feld "DTP"
Devices-Datei
Portselektor-Verbindung, 610
Feld "expect" des Felds "Chat Script", 601, 602
Feld "ID-list" der Grades-Datei, 630, 631
Feld "Job-size" der Grades-Datei, 630
Feld "Line" der Devices-Datei, 607
Feld "Line2" der Devices-Datei, 607
Feld "Permit-type" der Grades-Datei, 630
Feld "Phone" der Systems-Datei, 601
Feld "Speed"
Devices-Datei, Feld "Class" und, 608
Systems-Datei, 600
Feld "System-job-grade" der Grades-Datei, 629, 630
Feld "System-Name" der Systems-Datei, 598
Feld "Time" der Systems-Datei, 599, 621
Feld "Type"
Devices-Datei, 606
Systems-Datei, 600
Feld "User-job-grade" der Grades-Datei, 629
fg-Option, mount-Befehl, 163
file too large (Meldung), 136
find-Befehl, suchen .rhosts-Dateien, 685
Firewalls
Dateisysteme über einhängen, 95
NFS-Zugriff über, 83
WebNFS-Zugriff über, 107
forcedirectio-Option, mount-Befehl, 163
.forward. *hostname*-Datei, 383
.forward-Dateien
deaktivieren, 340
für Benutzer, 382
Suchpfad ändern, 341
verwalten, 339
.forward+*detail*-Datei, 384
FPT-Archiv, WebNFS und, 105
Frame Relay, 430, 471
Freigabe von Dateisystemen, automatisch, 86
ftp-Befehl
Anmeldungen unterbrechen, 680
Remote-Anmeldungen authentifizieren, 689
Remote-Anmeldungen im Vergleich mit rlogin und rcp, 689
Remote-System-Verbindungen öffnen, 690, 691
FTP-Gastbenutzer, Einrichten, 656
FTP-Server, nowait, 671
ftp-Sitzungen
anonyme FTP-Konten, 689
Dateien kopieren
aus dem Remote-System, 691
in ein Remote-System, 693
Remote-System-Verbindungen öffnen, 691
Remote-System-Verbindungen schließen, 691
ftp-Unterbefehle, Beschreibung, 690
ftphosts, 655
fuser-Befehl, umountall-Befehl und, 170

G

g-Protokoll in Devices-Datei, 611
-G-Option, sendmail-Befehl, 404
-g-Option, lockd-Dämon, 148
geheimer Schlüssel, Datenbank, 210
Geheimer Schlüssel
Serverabsturz und, 211
vom Remote-Server löschen, 211
Gemeinsam genutztes Objekt pppoe.so, 564
Gemeinsam genutztes pppoe.so-Objekt, 567
Gemeinsame Nutzung von Dateisystemen aufheben, unshareall-Befehl, 178
Gemeinsamer Dateizugriff
Beispiele, 175
gemeinsam genutzte Dateien auf mehreren Servern replizieren, 121
gemeinsame Nutzung aufheben, 178
Lese- und Schreibzugriff, 175
mehrere Dateisysteme, 177–178
nicht authentifizierte Benutzer und, 173
nur gelistete Clients, 172
Root-Zugriff gewähren, 174
Sicherheitsprobleme, 171, 174, 208
Übersicht, 171

Gemeinsamer Dateizugriff *(Fortsetzung)*
Verbesserungen der NFS-Version 3, 78
Verbesserungen in NFS-Version 3, 81
Zugriff mit Schreibschutz, 171, 172, 175
`gen-etc-shells`-Skript, 342
`generic.m4`-Datei, 371
`generics_entire_domain` `FEATURE()`-Deklaration, 409
`genericstable` `FEATURE()`-Deklaration, 411
Gerätetyp für eine Kommunikationsverbindung, 600
`get`-Befehl (FTP), Beispiel, 692
`getfacl`-Befehl, NFS und, 198
`gethostbyname`-Befehl, 388
Gewichtung von Servern in Maps, 226
Gleichheitszeichen (=) im Wählcodekürzel, 601
Gleichsetzungen für Delivery Agents ab Version 8.12, `sendmail`-Befehl, 412
`GRACE_PERIOD`-Parameter, `lockd`-Dämon, 148
`Grades`-Datei
Beschreibung, 583, 628
Feld "ID-list", 630, 631
Feld "Job-size", 630
Feld "Permit-type", 630
Feld "System-job-grade", 629, 630
Feld "User-job-grade", 629
Schlüsselwörter, 630
Standardklasse, 630
Große Dateien
Erstellung von deaktivieren, 93
NFS-Unterstützung, 81
Übersicht, 205
GSS-API, und NFS, 82

H

`-h`-Option, `umountall`-Befehl, 170
hängende Programme, 138
`hard`-Option, `mount`-Befehl, 166
Hardware
Flusskontrolle
`Dialers`-Datei, 615
`Systems`-Datei, 604
UUCP
Konfigurationen, 579
Hardware, UUCP *(Fortsetzung)*
Portselektor, 606
Hardware für die Flusskontrolle
`Dialers`-Datei, 615
`Systems`-Datei, 604
`helpfile`-Datei, 369
`sendmail`-Befehl, 418
hierarchical mountpoints (Meldung), 133
Hierarchische Einhängepunkte (mehrere Einhängepunkte), 222
Hinauswahlrechner
adressieren
dynamisch, 556
Adressierung
statisch, 557
Definition, 426
eine serielle Verbindung konfigurieren mit `/etc/ppp/options.`*ttyname*, 532
einen Chat-Skript erstellen, 461
konfigurieren
CHAP-Authentifizierung, 490, 492–493
Kommunikation über eine serielle Verbindung, 460
Modem, 458–459
PAP-Authentifizierung, 483–484
serieller Port, 458–459
Verbindung mit einem Peer, 462–463
Planungsinformationen, 438
Remote-Peer aufrufen, 469–470
Übersicht der Schritte zum Konfigurieren, 456–457
`/home` Einhängepunkt, 213
`/home`-Einhängepunkt, 214
`/home`-Verzeichnis und NFS-Server einrichten, 116
HOST-Map-Variable, 227
host not responding (Meldung), 133
`hostname.`*interface*-Datei, NCA und, 63
Hosts
alle Dateisysteme aushängen aus, 170
Antwort prüfen von, 704
in `/etc/hosts.equiv` Datei, 682
in `/etc/hosts.equiv`-Datei, 681
Pakete senden an, 704
Paketen senden an, 704
`hosts`-Datei, 63

hosts.equiv-Datei, 681, 682
hsfs-Option, autofs-Maps, 114
HTML-Datei, WebNFS und, 106
httpd-Befehl
  NCA und, 64–65
  Zugriff über eine Firewall und WebNFS, 107

I

ICMP-Protokoll, 706
IGMP-Protokoll, 706
ignoring invalid option (Meldung), 138
in.comsat-Dämon, 373
in.uucpd-Dämon, 581
index-Option
  bad argument (Fehlermeldung), 135
  in dfstab-Datei, 88
  WebNFS und, 106
  without public option (Fehlermeldung), 135
Indirekte Maps (autofs)
  Beispiel, 217, 218
  Beschreibung, 110
  Kommentare in, 217
  modifizieren, 112
  Syntax, 217
indirekte Maps (autofs), Übersicht, 217
Indirekte Maps (autofs)
  Übersicht, 218
  wann das Ausführen erforderlich ist automount-Befehl, 111
Indirekte Remote-Anmeldungen, 683
indirekte Remote-Anmeldungen, 683
inetd-Dämon, in.uucpd aufgerufen durch, 581
init-Befehl, PPP und, 475
-intr-Option, mount-Befehl, 125
IP-Routing-Tabelle, 708
IPv6-Adressen und Version 8.12, sendmail-Befehl, 418
ISDN über eine PPP-Verbindung, 428

K

K-Escape-Zeichen, Dialers-Datei, 614
-k-Option, umountall-Befehl, 170
KERB-Authentifizierung, NFS und, 82
Kernel, Erreichbarkeit des Servers prüfen, 126
/kernel/fs-Datei, prüfen, 142
keylogin-Befehl
  Secure NFS aktivieren, 103
  Sicherheitsprobleme bei der Remote-Anmeldung, 212
keylogout-Befehl, sicheres NFS und, 212
keyserv-Dämon, Secure NFS aktivieren, 103
Knotenname
  UUCP-Alias, 583, 621
  UUCP-Remote-Computer, 598, 618
Kollisionsquote (Netzwerk), 706
Kommentare
  in der Master-Map (auto_master), 214
  in direkten Maps, 216
  in indirekten Maps, 217
Kompilierungsflags, sendmail-Befehl, 352
Konfigurationsaufgaben für PPP
  Authentifizierung, 477–478
  Einwahlverbindung, 455
  Konfigurationsprobleme diagnostizieren, 514
  PPPoE-Tunnel, 495
Konfigurationsbeispiele für PPP
  CHAP-Authentifizierung, 448
  Einwahlverbindung, 440
  PAP-Authentifizierung, 446
  PPPoE-Tunnel, 452
  Standleitungsverbindung, 443
Konfigurationsdateien
  sendmail-Befehl, 378
  UUCP, 628
Konfigurationsschritte für PPP, Standleitungen, 471
Konfigurieren
  asppp-Verbindungen mit UUCP-Datenbanken, 584
  Mailgateways, 365
  UUCP
    Datenbankdateien, 584
    Hinzufügen von Anmeldungen, 586, 587
    Shell-Skripten, 587, 589
    TCP/IP-Netzwerke, 589, 590
Konfigurieren für die PAP-Authentifizierung, 480, 483–484, 484, 486

Konsolidieren von projektbezogenen Dateien, 117
Kopieren von Dateien (Remote)
  mit ftp, 690
  mit rcp, 695, 700

L

-L *tag*-Option, sendmail-Befehl, 404
-l Option, cu Befehl, 592
-l-Option, umountall-Befehl, 170
largefiles-Option
  Fehlermeldung, 138
  mount-Befehl, 164
LCK-UUCP-Sperrdateien, 633
LDAP ab Version 8.12, sendmail-Befehl und, 414
ldap_routing FEATURE()-Deklaration, 409
leading space in map entry (Meldung), 132
Lebensdauer der Registrierung (SLP), 246
Leerzeichen-Escape-Zeichen, 614
Lese- und Schreibzugriff
  Dateisysteme einhängen mit, 166
  Dateisysteme gemeinsam nutzen, 172
libslp.so-Bibliothek, 240
Limits-Datei
  Beschreibung, 583, 632
  Format, 632
Liste der Aufgaben, NCA, 51–52
LOCAL_DOMAIN() m4-Konfigurationsmakro, 408
local-host-names-Datei, 369, 418
local_lmtp FEATURE()-Deklaration, 409
local_no_masquerade FEATURE()-Deklaration, 409
local-Option (PPP), 475
lockd-Dämon, 148–149
LOCKD_GRACE_PERIOD-Parameter, lockd-Dämon, 148
LOCKD_RETRANSMIT_TIMEOUT-Parameter,
  lockd-Dämon, 148
LOCKD_SERVERS-Parameter, lockd-Dämon, 148
log-Option
  in dfstab-Datei, 89
  share-Befehl, 173
login- Option (PPP), in /etc/ppp/pap-secrets, 485
login-Befehl, sicheres NFS und, 212
login-Option (PPP)
  in /etc/ppp/options für einen Einwahlserver, 482
login-Option (PPP) *(Fortsetzung)*
  in /etc/ppp/pap-secrets, 552
LOGNAME Permissions-Datei
  Anmelde-IDs für Remote-Computer, 620
  Beschreibung, 619
  Kombinieren mit MACHINE, 627
  SENDFILES-Option, 620
  VALIDATE-Option, 626
LOGNAMEPermissions-Datei,
  VALIDATE-Option, 625
Lokale Dateien, autofs-Maps aktualisieren, 110
Lokale Dateisysteme, Gruppen aushängen, 170
Lokale Mailadressen, 361
Lokale Mailaliasdatei, Einrichten, 331
Lokaler Cache und NFS-Version 3, 78
Lokaler Delivery Agent, Mailservices, 356
Lokales Netzwerk (LAN), UUCP-Konfiguration, 580
lookupdotdomain FEATURE()-Deklaration, 410
Löschen, .rhosts-Dateien, 683
ls-Befehl, Zugriffssteuerungslisteneinträge und, 198

M

m4-Verzeichnis, 371
MACHINE Permissions-Datei
  Beschreibung, 620
  COMMANDS-Option, 623
  Kombinieren mit LOGNAME, 627
  OTHER-Option, 626
  standardmäßige Berechtigungen oder
    Beschränkungen, 620
MACHINEPermissions-Datei,
  COMMANDS-Option, 625
Mail-Aliasdateien
  Beschreibung, 379
  /etc/mail/aliases-Datei, 380
  .mailrc Aliase, 379
mail_aliases-NIS+-Tabelle, Einträge bearbeiten
  in, 329
mail-Befehl, 367
Mail-Benutzeragenten, 356
Mail.rc-Datei, 368
Mail-Routing, Mailadressen und, 386
Mail Transfer Agents, 356

Mailaateways, Definition, 365
Mailadressen
  % in, 361
  Beschreibung, 358
  Domains und Teildomains, 358
  lokal, 361
  Mail-Routing und, 386
  Unterscheidung zwischen Groß- und Kleinschreibung, 359
Mailaliasdateien, verwalten, 323
Mailbefehle, Interaktionen von, 374
Mailbox-Namen, 361
Mailboxen
  Dateien für, 361, 373
  Mail-Server und, 365
  Mailserver und, 365
  Speicherplatzbedarf, 365
Mailclients
  Definition, 365
  einen Mailclient einrichten, 307
  über NFS eingehängte Dateisysteme und, 307
`mailcompat`-Filter, 367
Maildomains
  Name Service-Domains und, 388
  `sendmail.cf`-Datei und, 387
Mailer
  Definition, 356
  integriert (`sendmail`)
    `[TCP]` und `[IPC]`, 416
  SMTP-Mailer (Simple Mail Transfer Protocol), 357
  Solaris-Mailer, 356, 357
  UUCP-Mailer (UNIX-to-UNIX Copy Command), 357
MAILER-DAEMON-Meldungen, 347
`MAILER()`-Deklarationen ab Version 8.12, 411
`mailer`-Verzeichnis, 371
Mailfilter-API`MILTER`, 354
Mailgateways
  einen Mailgateway einrichten, 310
  konfigurieren, 365
  prüfen, 344
  `sendmail.cf`-Datei und, 365
Mailhosts
  Beschreibung, 364
Mailhosts *(Fortsetzung)*
  einen Mailhost einrichten, 309
Mailkonfiguration
  lokale Mails und eine Remote-Verbindung, 302
  nur lokal, 301
  prüfen, 343
  typisch, 296
`mailq`-Befehl, 367
`.mailrc` Aliase, 379
`.mailrc`-Datei, 363
Mailserver, 365
  Beschreibung, 364
  Mailboxen auf, 361, 365
  Mailserver einrichten, 339
  Sicherung und, 365
  Speicherplatzbedarf für, 365
Mailservices
  Änderungen an `sendmail` ab Version 8.12, 400
  Änderungen an `sendmail` in Version 8.13, 392–400
  Hardwarekomponenten
    erforderliche Elemente, 363
    Mailclient, 365
    Mailgateway, 365
    Mailhost, 364
    Mailserver, 364
  Planen Ihres Mailsystems, 301
  Softwarekomponenten, 355
    lokaler Delivery Agent, 356
    Mail-Benutzeragent, 356
    Mail Transfer Agent, 356
    Mailadressen, 358
    Mailaliase, 362
    Mailbox-Dateien, 361
    Mailer, 356
  Übersicht der Schritte
    umfassende Übersicht der Schritte, 299
  Übersichten der Schritte
    Fehlerbehebungsverfahren und Tipps, 342
    `.forward`-Dateien verwalten, 339
    Mailaliasdateien verwalten, 323
    Mailservices einrichten, 304
    Warteschlangenverzeichnisse verwalten, 336
`mailstats`-Befehl, 368
Mailverbindungen mit anderen Systemen, prüfen, 346

Mailwarteschlange
einen Teil ausführen, 338
Mailwarteschlange ausführen, 339
Mailwarteschlange verschieben, 338
Verarbeitung der Mailwarteschlange erzwingen, 337
Warteschlangenverzeichnisse verwalten, 336
mailx-Befehl, 368
mailx.rc-Datei, 368
main.cf-Datei, 369, 370, 378
main.mc-Datei, 370, 417
main-v7sun.mc-Datei, 371, 417
Makefile-Datei, 370
makemap-Befehl, 373
Makros ab Version 8.12
definierte Makros (sendmail), 405
m4-Konfigurationsmakros (sendmail), 408
MAX-Makros (sendmail), 407
Map für öffentliche Schlüssel
DH-Authentifizierung, 210
Secure NFS aktivieren, 103
map key bad (Meldung), 133
Map-Variable für den Prozessortyp, 227
Maps (autofs)
Arten und Verwendung, 110
ausführbar, 229
automount-Befehl
Zeitpunkt der Ausführung, 111
Bezugnahme auf andere Maps, 228, 229
direkte, 215, 216
Einhängekonflikte vermeiden, 112
indirekte, 217, 218
Kommentare in, 214, 216, 217
lange Zeilen aufteilen in, 214, 216
Master, 213
mehrere Einhängepunkte, 222
modifizieren
direkte Maps, 112
indirekte Maps, 112
Master-Map, 111
Navigationsprozess starten, 221
Navigationsprozesse starten, 214
Netzwerknavigation, 220
Pflege, 110
Maps (autofs) *(Fortsetzung)*
schreibgeschützte Dateien für Clients auswählen, 223, 226
Sonderzeichen, 233
Variablen, 227
Verwaltungsaufgaben, 110
Zeilen aufteilen in, 217
MASQUERADE_EXCEPTION()
m4-Konfigurationsmakro, 408
Master-Map (auto_master)
/- Einhängepunkt, 213, 216
Beschreibung, 110
Inhalt, 213, 215
Kommentare in, 214
mit /etc/mnttab-Datei vergleichen, 219
modifizieren, 111
Sicherheitsbeschränkungen, 121
Syntax, 213
Übersicht, 213
vorinstalliert, 116
Master-Maps (auto_master)
Optionen außer Kraft setzen, 115
Secure NFS aktivieren, 104
Übersicht, 213
wann das Ausführen erforderlich istautomount-Befehl, 111
MAXBADCOMMANDS-Makro, sendmail-Befehl, 407
MAXETRNCOMMANDS-Makro, sendmail-Befehl, 407
MAXHELOCOMMANDS-Makro, sendmail-Befehl, 407
MAXNOOPCOMMANDS-Makro, sendmail-Befehl, 407
MAXVRFYCOMMANDS-Makro, sendmail-Befehl, 407
mconnect-Befehl, 346, 368
Mehrere Dateien (ftp), 691
Meldungen
UUCP
ASSERT-Fehlermeldungen, 635, 636
Prüfen von Fehlermeldungen, 594
STATUS-Fehlermeldungen, 636, 638
Meldungstypen, SLP, 288–289
mget-Befehl (FTP), Beispiel, 693
MILTER, Mailfilter-API, 354
Minuszeichen (–),
/etc/hosts.equiv-Dateisyntax, 681

Mit Schreibschutz
  Dateiauswahl durch autofs, 223, 226
  Dateisysteme einhängen, 167
  Dateisysteme einhängen mit, 166
mit Schreibschutz
  Dateisysteme gemeinsam nutzen, 172
Mit Schreibschutz
  Dateisysteme gemeinsam nutzen, 175
mit Schreibschutz
  Freigeben von Dateisystemen, 171
mnttab-Datei
  erstellen, 179
  mit der auto_master-Map vergleichen, 219
Modem, Modemprobleme beseitigen, 515
Modem (PPP)
  Chat-Skripten
    Beispiel, 461, 539–541, 542–543, 546
    für einen ISDN-TA, 545–546
    UNIX-basierte Anmeldung, 543–545
    Vorlage, 541–542
  Chat-Skripten erstellen, 538
  DSL, 436
  konfigurieren
    Einwahlserver, 464–465
    Hinauswahlrechner, 458–459
  Modemgeschwindigkeit einstellen, 465
Modem (UUCP)
  direkte Verbindung, 609
  Eigenschaften einstellen, 604, 615
  Fehlerbehebung, 592
  Portselektor-Verbindung, 610
  UUCP-Datenbanken
    Feld "Dialer-Token-Pairs" der Devices-Datei, 610
  UUCP-Datenbanken, Feld "DTP" Devices-Datei, 609
  UUCP-Datenbanken, Feld "DTP"Devices-Datei, 610
  UUCP-Hardwarekonfiguration, 580
Modifizieren
  direkte autofs-Map, 112
  indirekte autofs-Maps, 112
  Master-Map (auto_master), 111
mount-Befehl, 162–169
mount-Befehl *(Fortsetzung)*
  autofs und, 77
  Bedarf an Clients ohne lokalen Massenspeicher, 77
  Dateisysteme manuell einhängen, 92
  Erstellung von großen Dateien deaktivieren, 93
  Failover mit, 167
  mit NFS-URL, 96
  NFS-URL mit, 167
  Optionen
    Beschreibung, 163–166
    nolargefiles, 93
    ohne Argumente, 169
    public, 95
  verwenden, 167
mount of server:pathname (Fehler), 133
mountall-Befehl, 170
mountd-Dämon, 149
  Antwort des Servers prüfen, 127
  Betrieb prüfen, 129, 137
  nicht registriert mit rpcbind, 137
mounting, force direct I/O, 164
mput-Befehl (FTP), Beispiel, 695
mqueue-Verzeichnis, 373
MS-DOS-Dateien, mit autofs zugreifen, 114
Multicast (SLP)
  DAs, 254, 256
  Datenverkehr, 270
  Lebensdauereigenschaft, 258
  Multihomed-Rechner und, 274
  Schnittstellen ändern, 276
  Serviceanforderungen, 271
  Weitergabe, 260
  wenn deaktiviert, 275
Multihomed-Hosts (SLP)
  Bereiche und, 278
  deaktiviertes Unicast-Routing, 276
  Konfiguration, 274
  Nur-Broadcast-Routing, 261
  ohne Multicast, 271
  Proxy-Advertisement, 277–278
  Schnittstellen ändern, 276
MX-Datensätze (Mail Exchanger), 312
MYNAME-Option der Permissions-Datei, 621

N

n-Escape-Zeichen, Dialers-Datei, 614
N-Escape-Zeichen, Dialers-Datei, 614
Nachweise, RPC-Authentifizierungssystem, 209
name-Option (PPP)
  für die CHAP-Authentifizierung, 490
  in /etc/ppp/pap-secrets, 485
  mit noservice, 566
Name Service DNS, sendmail-Programm und, 312
Name Service-Domains, Maildomains und, 388
Name Services, Pflege von autofs-Maps, 110
Namen/Benennung
  Knotenname
    UUCP-Alias, 583
    UUCP-Remote-Computer, 598, 618
Namen/Benennungen
  Knotenname
    UUCP-Alias, 621
Namespaces
  auf gemeinsam genutzten zugreifen, 119
  autofs und, 84
Navigieren mit Maps
  Prozess starten, 221
  Übersicht, 220
Navigieren mithilfe von Maps, Prozess starten, 214
NCA
  aktivieren, 53–55
  Ändern der Protokollierung, 56
  Anforderungen, 52
  Architektur, 64–65
  Dateienbeschreibung, 63
  deaktivieren, 56
  httpd und, 64–65
  Kernel-Modul, 64–65
  Liste der Aufgaben, 51–52
  neue Funktionen, 50
  Socket-Bibliothek, 57
  Sockets, 52
  Übersicht, 49–50
nca_addr.so-Bibliothek, 64
nca_httpd_1.door-Datei, 64
nca.if-Datei, 53, 63
NCA-Protokolldatei, 64
ncab2clf-Befehl, 64
ncaconfd-Befehl, 64
ncakmod.conf-Datei, 54, 56, 63
ncakmod-Modul, 64–65
ncalogd.conf-Datei, 54, 56, 63
ncalogd-Skript, 63
ncaport.conf-Datei, 63
/net-Einhängepunkt, 214
net.slp.DAActiveDiscoveryInterval-Eigenschaft, 254
  Definition, 253
net.slp.DAAddresses-Eigenschaft, 256, 269, 274
  Definition, 253
net.slp.DAAttributes-Eigenschaft, 258
net.slp.DAHeartBeat-Eigenschaft, 256, 258
  Definition, 253
net.slp.interfaces-Eigenschaft
  DAs und, 273
  konfigurieren, 276
  Multihomed-Hosts und, 279
  nicht gesteuerte Schnittstellen und, 279
  Schnittstellen ändern, 277
net.slp.isBroadcastOnly -Eigenschaft, 262
net.slp.isBroadcastOnly-Eigenschaft, 261, 275, 276
net.slp.isDA (Eigenschaft), 252
net.slp.MTU (Eigenschaft), 260
net.slp.multicastTTL-Eigenschaft, 258
net.slp.passiveDADetection-Eigenschaft, 253
  Definition, 252
net.slp.randomWaitBound (Eigenschaft), 265
net.slp.serializedRegURL-Eigenschaft, 283
net.slp.useScopes-Eigenschaft, 268–269, 269, 285
  Definition, 267
netconfig-Datei, Beschreibung, 142
netstat-Befehl, 245, 705, 708
  -i-Option (Schnittstellen), 705, 706
  -r-Option (IP-Routing-Tabelle), 708
  -s-Option (pro Protokoll), 706
  Übersicht, 703, 705
Network Cache and Accelerator, *Siehe* NCA
Netzwerk-Sperren-manager, 81
Netzwerkauthentifizierung für
  Remote-Anmeldungen, 680, 682, 683
Netzwerkdatenbank-Services, UUCP-Port, 590
Netzwerke
  Anzeigen von Leistungsinformationen, 703

Netzwerke *(Fortsetzung)*
Befehle zum Überwachen der Leistung, 703
Clientaufrufe von Servern verfolgen, 703, 705
Fehlerbehebung
Hardwarekomponenten, 711
hohe Neuübertragungsrate, 709
Leistunginformationen anzeigen
Hostantwort, 704
Leistungsinformationen anzeigen, 704, 705, 711
Clientstatistiken, 709, 711
Hostantwort, 704
IP-Routing-Tabelle, 708
Kollisionsquote, 706
Schnittstellenstatistiken, 705, 708
Serverstatistiken, 709, 711
Pakete
abgeworfen, 705
an Hosts senden, 704
aus dem Netzwerk erfassen, 705
Fehlerquoten, 706
Prüfen der Zuverlässigkeit, 703
über das Netzwerk erfassen, 703
übertragene Anzahl, 706
Zuverlässigkeit prüfen, 704
Netzwerkschnittstellen (SLP), Überlegungen, 279
`newaliases` Befehl, UUCP und, 591
`newaliases`-Verknüpfung, 373
`newkey`-Befehl, Secure NFS aktivieren, 102
NFS
Befehle, 160
-Dämonen, 147–160
Versionsaushandlung, 187–188
NFS-ACL
Beschreibung, 80, 197–199
NFS ACL, Fehlermeldung, `Permission denied`, 139
NFS-Administration, Verantwortlichkeit des Administrators, 86
`NFS can't support nolargefiles` (Meldung), 138
NFS_CLIENT_VERSMAX (Schlüsselwort), 144
NFS-Clients
NFS-Services, 75
nicht kompatible Betriebssysteme unterstützen, 120
NFS-Fehlerbehebung
feststellen, an welchem Punkt der NFS-Service ausgefallen ist, 129
hängende Programme, 138
Remote-Einhängungsprobleme, 137
Serverprobleme, 126
Strategien, 124
NFS-Server
aktuelle Informationen sammeln, 130
Auswahl von Dateien durch autofs, 226
Fehlerbehebung
Probleme beheben, 126
Remote-Einhängeprobleme, 125
Remote-Einhängungsprobleme, 137
für das Remote-Einhänen erforderliche Dämonen, 124
gemeinsam genutzte Dateien replizieren, 121
Gewichtung in Maps, 226
verwalten, 86
NFS_SERVER_DELEGATION (Schlüsselwort), 144
NFS_SERVER_VERSMAX (Schlüsselwort), 144
NFS_SERVER_VERSMIN (Schlüsselwort), 144
NFS-Serverprotokollierung
aktivieren, 89–90
Übersicht, 83
NFS-Services
andere Versionen auf dem Client auswählen durch `/etc/default/nfs`-Datei ändern, 100–101
`mount`-Befehl verwenden, 101–102
andere Versionen auf dem Server auswählen, 99–100
Neustarten, 130
starten, 97–98
stoppen, 98
Übersicht der Schritte, 96
NFS-Sperrung, clientseitiges Failover und, 204
NFS-Umgebung, sicheres NFS-System, 208
NFS-URL
autofs und, 122
Dateisysteme einhängen mit, 95–96
einhängen mit, 83
`mount`-Befehl (Beispiel), 167
Syntax, 106–107
WebNFS und, 105

NFS V2 can't support largefiles (Meldung), 138
NFS-Version 4, Funktionen in, 188–199
nfs4cbd-Dämon, 149
nfscast: cannot receive reply (Meldung), 134
nfscast: cannot send packet (Meldung), 134
nfscast: select (Meldung), 134
nfsd-Dämon, 150
  Antwort des Servers prüfen, 127
  einhängen und, 201–202
nfsd Dämon, Betrieb prüfen, 129
nfslog.conf-Datei
  Beschreibung, 145–147
  NFS-Serverprotokollierung aktivieren, 89
nfslogd-Dämon
  Beschreibung, 150–151
  NFS-Serverprotokollierung aktivieren, 90
nfslogd-Datei, 144–145
nfsmapid-Dämon
  ACLs und, 197–199
  Beschreibung, 78, 151–159
  DNS-TXT-Datensätze und, 154–155
  Konfigurationsdateien und, 153
  NFSv4-Domain ermitteln, 155–156
  NFSv4-Standarddomain konfigurieren, 156–159
  Vorrangsregeln und, 153–154
  zusätzliche Informationen zu, 159
nfsmapid_domain (Parameter), 152
NFSMAPID_DOMAIN (Schlüsselwort), 144, 198
nfsstat-Befehl, 130, 179–181, 709, 711
  -c-Option (Clients), 709
  -m-Option (pro Dateisystem), 709, 711
  -s-Option (Server), 709
  Übersicht, 703, 709
Nicht übermittelte Mail, Fehlerbehebung, 344
Nicht zugeordnete Benutzer- oder Gruppen-IDs, prüfen auf, 199
NIS+-mail_aliases-Tabelle
  Aliase einfügen in, 327
  einen einzelnen Eintrag auflisten aus, 326
  Einträge durch Bearbeiten einfügen, 328
  Einträge löschen aus, 329
  gesamten Inhalt auflisten, 326
  Tabellen initiieren, 325
  teilweise Entsprechungen auflisten, 326
NIS+-Name Service, autofs-Maps aktualisieren, 110
NIS+-Tabelle mail_aliases, 382
NIS-mail.aliases-Map, Einrichten, 330
NIS-Name Service, autofs-Maps aktualisieren, 110
nisaddcred-Befehl, Secure NFS aktivieren, 102
nistbladm-Befehl
  autofs-Map modifizieren(auto_master), 111
  direkte autofs-Map modifizieren, 112
  indirekte autofs-Maps modifizieren, 112
nnn-Escape-Zeichen, 614
no_default_msa FEATURE()-Deklaration, 410
no info (Meldung), 134
No such file or directory (Meldung), 137
noauth Option (PPP), 475
noauth-Option (PPP), 463
nocanonify FEATURE()-Deklaration, 410
noccp-Option (PPP), 467
noipdefault-Option (PPP), 463
nolargefiles-Option
  Fehlermeldung, 138
  in vfstab-Datei, 93
  mount-Befehl, 93, 164
NOREAD-Option der Permissions-Datei, 622
noservice-Option (PPP), 566
nosuid-Option, share-Befehl, 173
Not a directory (Meldung), 133
Not found (Meldung), 132
nouucp FEATURE()-Deklaration, 410
NOWRITE-Option der Permissions-Datei, 622
nsswitch.conf-Datei, 312, 681
nthreads-Option, lockd-Dämon, 148
NTP-Client, einrichten, 68
ntp.conf-Datei, 68
NTP-Dateien, 70
NTP-Server, einrichten, 68
ntpdate-Befehl, 70
ntpq-Befehl, 70
ntpstats-Verzeichnis, 70
ntptrace-Befehl, 70
Null-Escape-Zeichen, 614
nullclient FEATURE()-Deklaration, 410
Nummernzeichen (#)
  Kommentare in der Master-Map (auto_master), 214

Nummernzeichen (#) *(Fortsetzung)*
Kommentare in direkten Maps, 216
Kommentare in indirekten Maps, 217

O

-O-Option, mount-Befehl, 167
-o-Option
mount-Befehl, 167
share-Befehl, 172, 175
Öffnen von Remote-System-Verbindungen, 690, 691
Oktalzahlen-Escape-Zeichen, 614
OPEN-Unterstützung zur gemeinsamen Nutzung, NFS-Version 4, 195
openssl-Befehl und sendmail, 318
Optimierung der SLP-Leistung, 257
Option (PPP)
local, 475
noauth, 475
Optionen (PPP)
Analyse mihilfe des pppd-Dämons, 527
asyncmap, 532
auth, 482
call, 470, 535
connect, 463, 546
crtscts, 460
Fehlersuche, 508
init, 475, 532
login, 482, 552
name, 485
noauth, 463
noccp, 467
noipdefault, 463
noservice, 566
Optionsberechtigungen, 528
passive, 475
persist, 475
Richtlinien zur Verwendung, 525–533
sync, 475
xonxoff, 468
Optionen für gemeinsamen Dateizugriff, 172
Optionen im sendmail-Befehl
Befehlszeilenoptionen ab Version 8.12, 402, 403
Optionen in sendmail-Befehl
Befehlszeilenoptionen ab Version 8.12, 404
Befehlszeilenoptionen in Version 8.13, 397–398
Konfigurationsdateioptionen in Version 8.13, 398–399
PidFile-Option, 404
ProcessTitlePrefix-Option, 404
options-Datei, in PPP, 460
options.*ttyname*-Datei(PPP), *Siehe* /etc/ppp/options.*ttyname*
OSNAME-Map-Variable, 227
OSREL-Map-Variable, 227
ostype-Verzeichnis, 371
OSVERS-Map-Variable, 227
OTHER-Option der Permissions-Datei, 626
owner-, Präfix und Mailbox-Namen, 361
owner- Präfix, Mailalias mit, 362
owner-owner und Mailbox-Namen, 361

P

p-Escape-Zeichen, Dialers-Datei, 614
Paketgröße, für SLP konfigurieren, 260
PAP (Password Authentication Protocol)
Beispielkonfiguration, 446
Datenbank für PAP-Berechtigungsnachweise erstellen, 480–481
Definition, 549
Empfehlungen für Passwörter, 550
/etc/ppp/pap-secrets-Datei, 549
konfigurieren
auf einem Einwahlserver, 481–483
vertrauenswürdige Anrufer, 483–484, 484, 486
login-Option verwenden, 552
PAP (Password Authentication Protocol)
Authentifizierungsprozess, 550
Planung, 478
Übersicht der Schritte, 478–479
Parität
Dialers-Datei, 616
Systems-Datei, 604
passive-Option (PPP), 475
Passiver Modus, 621

passwd-Datei, Aktivieren von
UUCP-Anmeldungen, 586
Passwörter
Authentifizierung für Remote-Anmeldungen
ftp-Befehl, 689, 690
rlogin-Befehl, 680, 683, 687
autofs und Superuser-Passwörter, 77
DH-Passwortschutz, 209
Erstellung eines sicheren RPC-Passworts, 102
UUCP, privilegiert, 625, 626
pathconf: no info (Meldung), 134
pathconf: server not responding (Meldung), 134
PC-DOS-Dateien, mit autofs zugreifen, 114
pcfs-Option, autofs-Maps, 114
Peer
Authentifizierer, 432
peer, Authentifizierungsempfänger, 432
Peer
Definition, 425
Einwahlserver, 426
Hinauswahlrechner, 426
PPPoE-Client, 434, 450
Standleitungs-Peer, 430
Zugangsserver, 434, 451
penril-Eintrag in Dialers-Datei, 614
Perl 5, Einführung, 46–47
Permission denied (Meldung), 137
Permissions-Datei
Beschreibung, 583, 619
CALLBACK-Option, 623
COMMANDS-Option, 623, 625, 627
Dateiübertragungsberechtigungen, 620, 623
Einrichten der Sicherheit, 590
Format, 619
Knotennamen ändern, 621
LOGNAME
Anmelde-IDs für Remote-Computer, 620
Beschreibung, 619
Kombinieren mit MACHINE, 627
MACHINE
Beschreibung, 620
Kombinieren mit LOGNAME, 627
OTHER-Option, 626
Permissions-Datei, MACHINE *(Fortsetzung)*
standardmäßige Berechtigungen oder Beschränkungen, 620
MYNAME-Option, 621
NOREAD-Option, 622
NOWRITE-Option, 622
OTHER-Option, 626
READ-Option, 622
Remote-Ausführungsberechtigungen, 623, 626
REQUEST-Option, 620
Rückrufberechtigungen, 623
SENDFILES-Option, 620
Strukturierungseinträge, 619
Überlegungen, 620
uucheck-Befehl und, 582
uuxqt-Dämon und, 581
VALIDATE-Option, 625, 626
Weiterleitung, 627
WRITE-Option, 622
persist Option (PPP), 475
Pfadname
rcp-Befehl
absolute oder abgekürzte, 696
Pfadnamen
rcp-Befehl
absolute oder abgekürzte, 697
Syntaxoptionen, 697
Tilde (~) in, 696, 697
PidFile-Option, sendmail-Befehl, 404
ping-Befehl, 263, 686, 703, 704
Planungsdämon für UUCP, 581
Pluszeichen (+)
/etc/hosts.equiv-Dateisyntax, 681, 682
in autofs in Map-Namen, 228
in autofs-Map-Namen, 229
Point-to-Point Protocol, *Siehe* PPP
Poll-Datei
Beschreibung, 583, 628
Format, 628
Portmapper, einhängen und, 201–202
Ports
Devices-Dateieintrag, 607
UUCP, 590
Portselektorvariable in Devices-Datei, 606

postmaster-Alias, Erstellen, 333
Postmaster Mailbox, Beschreibung, 361
postmaster-Mailbox
  erstellen, 334
  prüfen, 344
PPP
  allgemeine Probleme, 506
  Authentifizierung, 431, 432
  Chat-Skript-Beispiele, 461
  Dateiberechtigungen, 528
  DSL-Unterstützung, 433
  ISDN-Unterstützung, 428
  Kompatibilität, 422
  Optionen für Konfigurationsdateien
    Siehe Optionen (PPP)
  pppd
    Siehe auch pppd-Befehl
  PPPoE, 434
  Probleme lösen
    Siehe auch PPP-Fehlerbehebung
  relevante RFCs, 424
  Ressourcen, externe, 423
  Standleitungsverbindung, 429
  Teile einer Verbindung, 425–431, 434–436
  Überblick, 421
  Übersicht der Konfigurationsdateien, 526
  Übersicht der Schritte für die PPP-Planung, 437
  Unterschied zu asppp, 423
  von Asynchronous PPP konvertieren, 575
  Wählverbindung, 425
PPP-Fehlerbehebung
  allgemeine Probleme, 506
    Authentifizierung, 523–524
    Chat-Skripten, 518, 519
    für Netzwerke, 512
    serielle Verbindungen, 519
    Standleitungsverbindungen, 523
  Diagnoseinformationen abrufen, 507–508, 508
  Übersicht der Schritte, 505
PPP-Fehlersuche
  allgemeine Probleme
    allgemeine Kommunikation, 513
    Chat-Skripten, 517
    mit der PPP-Konfiguration, 515
PPP-Fehlersuche *(Fortsetzung)*
  Fehlersuche aktivieren, 508
  Fehlersuche für Chat-Skripten, 516
  Kommunikationsprobleme beheben, 512
  Kommunikationsprobleme beseitigen, 514
  Modemprobleme beseitigen, 515
  Netzwerkprobleme diagnostizieren, 510
  PPPoE-Probleme diagnostizieren, 520
  Probleme mit der seriellen Verbindung diagnostizieren, 519
pppd-Befehl
  Analyseoptionen, 527
  Aufruf initiieren, 469
  Definition, 526
  Diagnose abrufen, 521
  Diagnoseinformationen abrufen, 507
  eine DSL-Leitung testen, 499
  Fehlersuche aktivieren, 508
pppdebug Protokolldatei, 521
PPPoE
  allgemeine Probleme beheben, 520, 521, 522
  Bereitstellen von Services über einen Zugangsserver, 562–564
  DSLAM, 436
  durch einen Zugangsserver Services bereitstellen, 564
  Liste von Befehlen und Dateien, 559
  Planen des Tunnels, 450
  Planung für den Tunnel, 452, 454
  snoop-Ablaufverfolgung abrufen, 522
  Übersicht, 434
  Übersichten der Schritte zum Konfigurieren, 495
  Zugangsserver konfigurieren, 500, 502
  Zugangsserver modifizieren, 501
PPPoE-Client
  Befehle, 567
  Dateien, 567
  Definition, 434
  /etc/ppp/peers/*peer-name*-Dateiverwendung (PPPoE), 568
  Geräte, 450
  konfigurieren, 497–498
  planen, 497
  Planung, 450

PPPoE-Client *(Fortsetzung)*
Übersicht der Schritte zum Konfigurieren, 495
Zugangsserver definieren, 498
Zugangsserver und, 568
`pppoec`-Dienstprogramm
Definition, 567
Diagnose abrufen, 521
`pppoed`-Dämon
Definition, 561
starten, 501
`.ppprc`-Datei
Berechtigungen, 528
Definition, 526
erstellen, 467
`praliases`-Befehl, 368
`preserve_local_plus_detail` `FEATURE()`-Deklaration, 410
`preserve_luser_host` `FEATURE()`-Deklaration, 410
Probleme mit Zugriffssteuerungslisten in NFS, vermeiden, 199
`ProcessTitlePrefix`-Option, `sendmail` Befehl, 404
Programme, hängend, 138
Projekte, Dateien konsolidieren, 117
Protokolldatei, für NCA, 64
Protokolldefinitionen in `Devices`-Datei, 611
Protokollebenen, `sendmail.cf` Datei, 379
Protokollieren, UUCP-Protokolldateien anzeigen, 581
Proxy-Advertisement (SLP), 281, 283
Proxy-Registrierung (SLP), Multihomed-Hosts, 277–278
Proxyregistrierung (SLP), 282, 284
Prozentzeichen (%) in Mailbox-Namen, 361
Prozessdiagramm, für CHAP, 554
Prüfen
Mailaliase, 344
prüfen, Mailkonfiguration, 343
Prüfen
Mailverbindungen mit anderen Systemen, 346
Regellisten, 345
Prüfen auf nicht zugeordnete Benutzer- oder Gruppen-IDs, 199
`pstack`-Befehl, 181–182
`public`-Option
Fehler beim gemeinsamen Zugriff (Meldung), 140
`public`-Option *(Fortsetzung)*
in `dfstab`-Datei, 88
`mount`-Befehl, 95, 166
WebNFS und, 105
Punkt (.)
`rcp`-Befehlssyntax, 698, 700
`put`-Befehl (FTP), Beispiel, 694

Q

`-qf`-Option, `sendmail`-Befehl, 404
`-qG`*name*-Option, `sendmail`-Befehl, 404
`-qp`*time*-Option, `sendmail`-Befehl, 404
`-q[!]I`*substring*-Option, `sendmail`-Befehl, 404
`-q[!]R`*substring*-Option, `sendmail`-Befehl, 404
`-q[!]S`*substring*-Option, `sendmail`-Befehl, 404
`-q` Option, `uustat` Befehl, 592
`queuegroup` `FEATURE()`-Deklaration, 410

R

r-Escape-Zeichen, `Dialers`-Datei, 614
`-r`-Option
`mount`-Befehl, 167
`umountall`-Befehl, 170
`-r` Option
`uucp` Befehl, 593
`Uutry` Befehl, 593
`rbl` `FEATURE()`-Deklaration, 411
`rcp`-Befehl, 695, 700
Beispiele, 700
Beschreibung, 695
Kopieren zwischen lokalen Systemen und Remote-Systemen, 700
`rcp` Befehl
Pfadnamen
absolut oder abgekürzt, 696
`rcp`-Befehl
Pfadnamen
absolut oder abgekürzt, 697
Syntaxoptionen, 697
`rcp` Befehl
Quelle und Ziel angeben, 696

rcp-Befehl
  Quelle und Ziel angeben, 697
  Sicherheitsprobleme, 696
  Verzeichnisse kopieren, 698
  zwischen lokalen und Remote-Systemen kopieren, 698
rdate-Befehl, 69
READ-Option der Permissions-Datei, 622
Regellisten
  prüfen, 345
  Version 8.12 von sendmail, 416
relay-domains-Datei, 369
relay_mail_from FEATURE()-Deklaration, 411
Remote-Anmeldungen
  authentifizierung (ftp), 689
  Authentifizierung (rlogin), 680, 683
    /etc/hosts.equiv-Datei, 681, 682
    Netzwerkauthentifizierung oder Remote-Systemauthentifizierung, 680, 681
    .rhosts-Dateien, 682, 683
  Betrieb eines Remote-Systems verifizieren, 686
  direkt oder indirekt (rlogin), 683
  direkte oder indirekt (rlogin), 683
  Domains, 680
  entfernen .rhosts-Dateien, 685
  feststellen, wer angemeldet ist, 686
  FPT-Verbindung öffnen, 690
  ftp-Befehle, 690
  FTP-Verbindung öffnen, 691
  FTP-Verbindung schließen, 691
  mit rlogin-Befehl, 687, 688
  sequentielle Anmeldungen, 683
  unterbrechen, 680
Remote-Ausführung (UUCP)
  Arbeitsdateien (C.), 633, 634
  Befehle, 620, 623, 626
  Dämon, 581
Remote-Dateisysteme
  Clients mit Dateisystemen auflisten, die per Remote-Zugriff eingehängt wurden, 178
  Gruppen aushängen, 170
Remote-Einhängen
  erforderliche Dämonen, 124
  Fehlerbehebung, 125, 129
Remote-Kopieren
  mit ftp, 690
  mit rcp, 695, 700
remote_mode FEATURE()-Deklaration, 411
Remote-Systeme
  abmelden (exit), 688
  abmelden(exit), 688
  anmelden, 680, 691
  Betrieb verifizieren, 686
  Definition, 643
  Remote-Kopieren
    mit rcp, 695, 700
  Remote-System, Dateien kopieren
    mit ftp-Befehl, 690
remote.unknown-Datei, 632
remount (Meldung), 132
replicas must have the same version, 139
replicated mounts must be read-only, 140
replicated mounts must not be soft, 140
Replizieren von gemeinsam genutzten Dateien auf mehreren Servern, 121
Replizierte Einhängungen, soft-Option und, 140
Repliziertes Dateisystem, 203–204
-request, Suffix und Mailbox-Namen, 361
REQUEST-Option der Permissions-Datei, 620
RFCs (Requests for Comments), PPP, 424
.rhosts-Dateien
  Beschreibung, 682
  löschen, 685
  Remote-Systemauthentifizierung, 681, 682–683
  Sicherheitsprobleme, 682, 683
  suchen, 685
rlogin-Befehl
  Anmeldungen unterbrechen, 680
  Authentifizierung, 680, 683
    /etc/hosts.equiv-Datei, 681, 682
    Netzwerkauthentifizierung oder Remote-Systemauthentifizierung, 680, 681
    .rhosts-Dateien, 682, 683
  Beschreibung, 680
  direkte oder indirekte Anmeldungen, 683
  mit, 687, 688
  Sicheres NFS und, 212
  Vorgang nach dem Anmelden, 684

rm-Befehl, 683
rmail-Befehl, 368
ro-Option
  mount-Befehl, 166
  mount-Befehl mit -o-Flag, 167
  share-Befehl, 172, 175
root-Option, share-Befehl, 174
Root-Verzeichnis, durch Clients ohne lokalen Massenspeicher einhängen, 77
Routine für den Zugriff auf öffentliche Dateien
  autofs und, 122
  einhängen und, 201
  NFS-Einhängung mit, 83
  WebNFS und, 105
RPC, 709
  Authentifizierung, 210
  sicher
    DH-Authentifizierungsprobleme, 211, 212
    Übersicht, 209
rpcbind-Dämon
  ausgefallen oder hängt, 137
  mountd-Dämon nicht registriert, 137
rpcinfo-Befehl, 182–184
RPCSEC_GSS, 82
RS-232-Telefonleitungen, UUCP-Konfiguration, 579
Rückruf
  CALLBACK-Option der Permissions-Datei, 623
  durch ein Chat-Skript aktivieren, 603
Rückschritt-Escape-Zeichen, 614
Rücksprung-Escape-Zeichen, 614
rusers-Befehl, 686
rw=client (Option), umountall-Befehl, 172
rw-Option
  mount-Befehl, 166
  share-Befehl, 172, 175

S

s-Escape-Zeichen, Dialers-Datei, 614
-s-Option, umountall-Befehl, 170
SA-Server (SLP), 265
SAs (SLP), 268, 276, 282
Schleifen, Aliase, 344
Schließen von Remote-System-Verbindungen, 691
Schlüsseldatei, NTP, 70
Schlüsselwort "Group" des Felds "Permit-type", 631
Schlüsselwort "Non-group" des Felds "Berechtigungstyp", 631
Schlüsselwort "Non-user" des Felds "Permit-type", 631
Schlüsselwort "User" des Felds "Permit-type", 631
Schlüsselwort ACU des Felds "Type", 606
Schlüsselwörter
  Devices-Datei, Feld "Type", 606
  Grades-Datei, 630, 631
  NFS-Versionsaushandlung, 187–188
Schnittstelle (PPP), HSI/P-Konfigurationsskript, 473
Schnittstellen (PPP)
  asynchrone Schnittstelle für PPP-Einwahl, 428
  asynchrone Schnittstelle für PPP-Hinauswahl, 427
  eine Schnittstelle auf PPPoE-Clients beschränken, 501
  einen PPPoE-Zugangsserver konfigurieren, 559
  für einen PPPoE-Client konfigurieren, 497–498
    Siehe auch /etc/ppp/pppoe.if-Datei
  für einen PPPoE-Zugangsserver konfigurieren, 500
  PPPoE-Schnittstellen mit /usr/sbin/sppptun anbinden, 560
  synchron für Standleitungen, 430
Schrägstrich (/)
  /- als Master-Map-Einhängepunkt, 213, 216
  Master-Map-Namen mit vorangestelltem, 213
  Root-Verzeichnis, durch Clients ohne lokalen Massenspeicher einhängen, 77
Schreibfehler, NFS und, 78
sec=dh-Option
  auto_master -Map, 104
  dfstab-Datei, 103
secrets-Datei für PPP, *Siehe* /etc/ppp/pap-secrets-Datei
Secure NFS-System
  DH-Authentifizierung und, 102
  Domainname, 102
  einrichten, 102
  verwalten, 102
Secure RPC, DH-Authentifizierungsprobleme, 211
SENDFILES-Option der Permissions-Datei, 620
sendmail-Befehl
  alternative Befehle, 354

sendmail-Befehl *(Fortsetzung)*
Änderungen ab Version 8.12, 400
Änderungen an Dateinamen oder Dateispeicherorten ab Version 8.12, 417
Änderungen in Version 8.13, 392–400
Befehlszeilenoptionen ab Version 8.12, 402, 403, 404
Befehlszeilenoptionen in Version 8.13, 397–398
Beschreibung, 375
Delivery Agent-Flags ab Version 8.12, 412
/etc/mail/helpfile-Datei, 418
/etc/mail/local-host-names-Datei, 418
/etc/mail/sendmail.ct-Datei, 418
/etc/mail/sendmail.cw-Datei, 418
/etc/mail/submit.cf, 401
/etc/mail/trusted-users-Datei, 418
FEATURE()-Deklarationen
Änderungen ab Version 8.12, 408
FEATURE()-Deklarationen ab 8.12
nicht unterstützt, 411
FEATURE()-Deklarationen ab Version 8.12
unterstützt, 408
FEATURE()-Deklarationen in Version 8.13, 399–400
Fehlermeldungen, 348
filename-Datei, 418
.forward-Dateien, 382
Funktionen der Warteschlange ab Version 8.12, 414
Funktionen und Merkmale von, 377
Gleichsetzungen für Delivery Agents ab Version 8.12, 412
helpfile-Datei, 418
Interaktionen mit NIS+ und DNS, 391
Interaktionen mit NIS und DNS, 389
Interaktionen von NIS+ und, 390
Interaktionen von NIS und, 389
IPv6-Adressen und Version 8.12, 418
Kompilierungsflags, 352
Konfigurationsdateioptionen in Version 8.13, 398–399
LDAP ab Version 8.12, 414
local-host-names-Datei, 418
Mailer, integriert
[TCP] und [IPC], 416
MAILER()-Deklarationen ab Version 8.12, 411
sendmail-Befehl *(Fortsetzung)*
main.mc-Datei, 417
main-v7sun.mc-Datei, 417
Makros
definierte Makros ab Version 8.12, 405
m4-Konfigurationsmakros ab Version 8.12, 408
MAX-Makros ab Version 8.12, 407
Name Services und, 387
NIS+-Tabelle mail_aliases, 382
NIS-Map aliases, 381
Regellisten ab Version 8.12, 416
sendmail.ct-Datei, 418
sendmail.cw-Datei, 418
submit.cf-Datei, 401
subsidiary.mc-Datei, 418
subsidiary-v7sun.mc-Datei, 418
TCP-Wrapper und, 401
trusted-users-Datei, 418
sendmail.cf-Datei, 369
alternative Konfiguration für, 322–323
Anbietereinstellung, 354
Beschreibung, 378–379
Konfigurationsdatei erstellen, 313
Maildomains und, 387
sendmail.cf Datei
Mailer, Beschreibung, 356
sendmail.cf-Datei
Mailgateways und, 365
Mailhosts und, 378
Mailserver und, 378
sendmail.cf Datei
Protokollebenen, 379
sendmail.cf-Datei
Versionsstand, 354
sendmail.ct-Datei, 418
sendmail.cw-Datei, 418
sendmail.hf-Datei, 418
sendmail.mc-Datei, 370
sendmail.pid-Datei, 369, 374
sendmail.st-Datei, *Siehe* statistics-Datei
sequenzielle Remote-Anmeldung, 683
Serieller Anschluss, auf einem Einwahlserver konfigurieren, 532

Serieller Port
konfigurieren
für einen Einwahlserver, 464–465
Hinauswahlrechner, 458–459
Serielles Aushängen, 170
Server
Siehe auch NFS-Server
Abstürze und geheime Schlüssel, 211
Auswahl von Dateien durch autofs, 223
Clientaufrufe verfolgen an, 703
Clientaufrufe verfolgen von, 705
Home-Verzeichnisserver einrichten, 116
Informationen anzeigen über, 703, 709, 711
NFS-Server und `vfstab`-Datei, 91
NFS-Services, 75
Server antwortet nicht (Meldung), Abbruch durch Tastaturbefehl, 125
server not responding (Meldung), 132, 134
hängende Programme, 138
Remote-Einhängungsprobleme, 137
Server und Clients, NFS-Service, 75
Service-Advertisement (SLP), 257, 283
Service-URLs
Proxyregistrierung (SLP), 282, 284
Serviceagent (SLP), 253, 257
Serviceanforderungen (SLP), 271
Serviceerkennung (SLP), 261, 263, 270
Services-Datenbank, UUCP-Port, 590
`setfacl`-Befehl, NFS und, 197
setgid-Modus, `share`-Befehl, 173
`setmnt`-Befehl, 179
setuid-Modus
`share`-Befehl, 173
Sicheres RPC und, 212
`share`-Befehl
Beschreibung, 171–177
Optionen, 172
Sicherheitsprobleme, 174
`shareall`-Befehl, 177–178
automatische gemeinsame Nutzung von Dateisystemen, 87
Einhängezugriff eines Clients deaktivieren, 95
NFS-Serverprotokollierung aktivieren, 89
WebNFS-Service aktivieren, 88
Shell-Skripten (UUCP), 587, 589
automatisch Ausführung, 587
manuelles Ausführen, 587
`uudemon.admin`, 589
`uudemon.cleanup`, 589
`uudemon.hour`
Beschreibung, 588
uudemon.hour
`uusched`-Dämonausführung durch, 581
`uuxqt`-Dämonausführung durch, 581
`uudemon.poll`, 588, 628
`showmount`-Befehl, 178
Sicheres Einhängen, `dfstab`-Dateioption, 103
sicheres NFS-System, Übersicht, 208
Sicheres RPC
DH-Authentifizierungsprobleme, 212
Übersicht, 209
Sicherheit
autofs-Beschränkungen anwenden, 121
DH-Authentifizierung
Benutzerauthentifizierung, 208
`dfstab`-Dateioption, 103
Passwortschutz, 209
Übersicht, 210, 211
`/etc/hosts.equiv`-Dateiprobleme, 682
NFS-Version 3 und, 78
Probleme beim gemeinsamen Dateizugriff, 171, 174
Probleme im Zusammenhang mit Kopiervorgängen, 696
`.rhosts`-Dateiprobleme, 682, 683, 685
Secure NFS-System
verwalten, 102
sicheres NFS-System
Übersicht, 208
sicheres RPC
DH-Authentifizierungsprobleme, 211
Sicheres RPC
DH-Authentifizierungsprobleme, 212
sicheres RPC
Übersicht, 209
UNIX-Authentifizierung, 208, 210
UUCP
COMMANDS-Option der `Permissions`-Datei, 623, 625

Sicherheit, UUCP *(Fortsetzung)*
Einrichten, 590
Sticky-Bit für Dateien in öffentlichen Verzeichnissen, 591
VALIDATE-Option der `Permissions`-Datei, 625, 626
Sicherheit und NFS
Beschreibung, 80, 197–199
Fehlermeldung, `Permission denied`, 139
Sicherheitsmodus und `mount`-Befehl, 166
Sicherheitsvarianten, 82
Sicherung, Mailserver und, 365
Skripten
Chat-Skripten (UUCP), 604
Escape-Zeichen, 602
Feld "expect", 601, 602
Format, 601
grundlegendes Skript, 602
Rückruf aktivieren, 603
Shell-Skripten (UUCP), 587, 589
UUCP-Shell-Skripten, 587
SLP
Advertisement, 271
Agenten und Prozesse, 238–240
analysieren `snoop`-SLP-Ablaufverfolgung, 246
Architektur, 237
Bereitstellung planen, 243–244
Broadcast-Routing, 261
Dämon, 240
Implementierung, 240
Konfigurationsdatei, 249, 250–251
Konfigurationseigenschaften, 250–251
konfigurieren, 243–244
Leistungsoptimierung, 257
Paketgröße, 260
protokollieren, 237
Suchanforderungen, 262
`slp.conf`-Datei, Kommentare, 251
`slp.jar`-Bibliothek, 240
SLP-Meldungstypen, 288–289
SLP-Statuscodes, 287–288
`slpd.conf`-Datei, 253, 268–269
`slpd`-Dämon, 281, 282, 286
Bereiche und, 268
`slpd`-Dämon *(Fortsetzung)*
DAs, 265
DAs entfernen, 256
Multihomed-Rechner und, 274
Proxy-Advertisement und, 277–278
SA-Server, 265
Schnittstellen ändern, 276
statische DAs und, 253
Takt, 255
SLPv2, Interoperabilität mit SLPv1, 271
`SMART_HOST()` `m4`-Konfigurationsmakro, 408
SMTP (Simple Mail Transfer Protocol)
Mailer, 357
`sendmail.cf`-Datei, 402
SMTP und TLS
aufgabenbezogene Informationen, 317–322
Beschreibung, 392–397
Konfigurationsdateioptionen für, 394–396
Makros für, 396
Regellisten für, 396–397
Sicherheitsüberlegungen zu, 397
`snoop`-Ablaufverfolgung, für PPPoE, 522
`snoop`-Befehl, 184, 703, 705
mehrere SLP-Anforderungen und, 276
mit SLP verwenden, 244, 246
Neuübertragung überwachen, 265
SLP-Datenverkehr und, 274
SLP-Serviceregistrierung und, 257
Sockets, NCA und, 52
`soft`-Option, `mount`-Befehl, 166
Solaris, UUCP-Version, 597
`solaris-antispam.m4`-Datei, 371
`solaris-generic.m4`-Datei, 340, 341, 371
Solaris PPP 4.0, *Siehe* PPP
`solaris2.m4`-Datei, 371
`solaris2.ml.m4`-Datei, 371
`solaris2.pre5.m4`-Datei, 371
`solaris8.m4`-Datei, 372
Sonderzeichen in Maps, 233
Sperren, Verbesserungen in NFS-Version 3, 81
spool (UUCP)
cleanup-Befehl, 581
Definitionen für Jobklassen, 628, 631

spool (UUCP) *(Fortsetzung)*
uusched-Dämon
Beschreibung, 581
maximale Anzahl von gleichzeitigen Ausführungen, 583
uusched Dämon
maximale gleichzeitige Ausführungen, 632
Verwaltungsdateien, 633, 634
Verzeichnis, 633
sppp-Einheitennummer, PPP-Adresszuweisung, 558
spray-Befehl, 703, 704
standardmäßiges Schlüsselwort des Felds "User-job-grade", 630
Standleitungsverbindung
allgemeine Probleme diagnostizieren
Netzwerk, 510
Übersicht, 523
Authentifizierung für die Verbindung, 432
Beispielkonfiguration, 443
CSU/DSU, 430
Definition, 429
demand-Skript, 475
eine synchrone Schnittstelle konfigurieren, 472–473
Hardware, 442
Kommunikationsprozess, 431
Konfiguration, 443
Medien, 430
planen, 442, 443, 445, 473–474
Teile der Verbindung, 429–430
Übersicht der Schritte zum Konfigurieren, 471
Starten
Aktivieren
Echoprüfung, 614
autofs-Service, 98
NFS-Services, 97–98
Rückruf durch ein Chat-Skript aktivieren, 603
UUCP-Shell-Skripten, 589
statd-Dämon, 159–160
Statische Adressierung, PPP, 557
statistics-Datei, 369
STATUS-Fehlermeldungen (UUCP), 594, 636, 638
.Status-Verzeichnis, 594
Statuscodes, SLP, 287–288
Sternchen (*), in autofs-Maps, 233
Sticky-Bit für Dateien in öffentlichen Verzeichnissen, 591
Stoppen
autofs-Service, 98
Deaktivieren
Echoprüfung, 614
NFS-Services, 98
STREAMS, Gerätekonfiguration, 631
STTY-Flusskontrolle, 604, 615
submit.cf-Datei, 369, 370, 401
submit.mc-Datei, 370
subsidiary.cf-Datei, 302, 369, 370
subsidiary.mc-Datei, 371, 418
subsidiary-v7sun.mc-Datei, 372, 418
Suchanforderungen (SLP), 262
Suchen
beim Remote-System angemeldete Benutzer, 686
mit einer NFS-URL, 106–107
suchen, .rhosts-Dateien, 685
sun_reverse_alias_files FEATURE()-Deklaration, 411
sun_reverse_alias_nis FEATURE()-Deklaration, 411
sun_reverse_alias_nisplus FEATURE()-Deklaration, 411
Superuser, autofs und Passwörter, 77
sync-Option (PPP), 475
synchrones PPP
Siehe Standleitungsverbindung
synchrone Geräte konfigurieren, 472
Synchronisieren der Zeit, 211
mit einem anderen System, 69
Sys-Name-Variable des Felds "Type", 606
Sysfiles-Datei
Beispiele, 618
Beschreibung, 583, 617
Format, 618
Systems-Liste ausgeben, 618
syslog.conf-Datei, 346
syslogd-Befehl, 373
Sysname-Datei, 583, 618
Systemauthentifizierung für Remote-Anmeldungen, 680, 681
Systems-Datei
Beschreibung, 583, 597

Systems-Datei *(Fortsetzung)*
Devices-Datei, Feld "Class" und, 608
Devices-Datei, Feld "Type" und, 606
Escape-Zeichen, 602
Fehlerbehebung, 594
Feld "Chat Script", 601, 604
Feld "Phone", 601
Feld "Speed", 600
Feld "System-Name", 598
Feld "Time"
Beschreibung, 599
Eintrag Never, 621
Feld "Type", 600
Format, 598
Hardware-Flusskontrolle, 604
mehrere oder verschiedene Dateien, 583, 597, 617
Parität einstellen, 604
TCP/IP-Konfiguration, 589, 590
Wählcodekürzel, 583, 601

T

T-Escape-Zeichen
Devices-Datei, 610
Dialers-Datei, 610, 614
t-Protokoll in Devices-Datei, 611
-t-Option, lockd-Dämon, 148
Tag-Einträge des Felds "Time", 599
TCP, NFS-Version 3 und, 80
TCP/IP-Netzwerke
UUCP über, 589, 590
TCP/IP-Verkehr, 703, 705, 706
TCP-Protokoll, 706
TCP-Wrapper, sendmail-Befehl und, 401
Telefonleitungen, UUCP-Konfiguration, 580
Telefonnummern in Systems-Datei, 601
telnet-Befehl, sicheres NFS und, 212
temporäre (TM) UUCP-Datendateien, 633
Temporäre Dateizugriffsroutinen, NFS-Version 4, 191–192
Testen, Paketzuverlässigkeit, 703
Tilde (~)
abgekürzte Pfadnamen, 696, 697
rcp-Befehlssyntax, 698, 700
TLS (Transport Layer Security) und SMTP
aufgabenbezogene Informationen, 317–322
Beschreibung, 392–397
Konfigurationsdateioptionen für, 394–396
Makros für, 396
Regellisten für, 396–397
Sicherheitsüberlegungen zu, 397
TLS und SMTP
aufgabenbezogene Informationen, 317–322
Beschreibung, 392–397
Konfigurationsdateioptionen für, 394–396
Makros für, 396
Regellisten für, 396–397
Sicherheitsüberlegungen zu, 397
TM UUCP, temporäre Datendateien, 633
Token (Dialer-Token-Paare), 608, 610
transport setup problem, Fehlermeldung, 135
Transportprotokoll, NFS-Aushandlung, 199–200
truss-Befehl, 185
trusted-users-Datei, 369, 418
Tunnel
Beispielkonfiguration, 452, 454
Definition (PPP), 434
Übersichten der Schritte zum Konfigurieren, 495

U

-U-Option, sendmail-Befehl, 404
UAs, Anforderungen, 257
UAs (SLP), 245, 271
Zeitüberschreitung bei Anforderungen, 273
Über NFS eingehängte Dateisysteme
Mailclients und, 304, 307
Mailserver und, 305
Überlagern eines bereits eingehängten Dateisystems, 167
Übertragungsgeschwindigkeit für eine UUCP-Kommunikationsverbindung, 600, 608
Übertragungsgeschwindigkeit für UUCP-Kommunikationsverbindung, 600
Übertragungsprotokolle für Geräte, 611
UDP, NFS und, 80–81
UDP-Protokoll, 706
UDP/TCP-Unicast (SLP), 274

Umgekehrter Schrägstrich (\) in Maps, 214, 216, 217
Umgekehrter Schrägstrich (Escape-Zeichen)
  Dialers-Datei, Sendezeichenfolgen, 613
  Systems-Datei, Chat-Skript, 602
umount Befehl, autofs und, 77
umount-Befehl, Beschreibung, 169–170
umountall-Befehl, 170–171
uname -n-Befehl, 618
Und-Zeichen (&), in autofs-Maps, 232
Unicast-Routing (SLP), 274
  deaktiviert, 276
UNIX-Authentifizierung, 208, 210
unshare-Befehl, 177
unshareall-Befehl, 178
Unterbrechen von Remote-Anmeldungen, 680
Unterfeld "retry" des Felds "Time", 599
Unterstrich (_) in Mailbox-Namen, 361
URL-Servicetypen, WebNFS und, 106
Usenet, 579, 597
/usr/bin/aliasadm-Befehl, 367
/usr/bin/cu -efehl, Systems-Listen ausgeben, 618
/usr/bin/cu-Befehl
  Beschreibung, 582
  mehrere oder verschiedene Konfigurationsdateien, 583, 617
/usr/bin/cu Befehl, Überprüfen von Modems oder ACUs, 592
/usr/bin/mail-Befehl, 367
/usr/bin/mailcompat-Filter, 367
/usr/bin/mailq-Befehl, 367
/usr/bin/mailstats-Befehl, 368
/usr/bin/mailx-Befehl, 368
/usr/bin/mconnect-Befehl, 346, 368
/usr/bin/ncab2clf-Befehl, 64
/usr/bin/praliases-Befehl, 368
/usr/bin/rmail-Befehl, 368
/usr/bin/uucp Befehl
  Berechtigungen für die Weiterleitung, 627
/usr/bin/uucp-Befehl
  Beschreibung, 582
  Home-Verzeichnis der Anmelde-ID, 581
/usr/bin/uucp Befehl
  Suche nach Übertragungsfehlern, 593
/usr/bin/uucp-Befehl
  uucico-Ausführung durch, 580
/usr/bin/uulog Befehl, 595
/usr/bin/uulog-Befehl, 581
/usr/bin/uupick Befehl, 592
/usr/bin/uupick-Befehl, 582
/usr/bin/uustat Befehl, 592
/usr/bin/uustat-Befehl, 582
/usr/bin/uuto-Befehl
  Beschreibung, 582
/usr/bin/uuto Befehl, Entfernen von Dateien aus dem öffentlichen Verzeichnis, 592
/usr/bin/uuto-Befehl
  uucico-Ausführung durch, 580
/usr/bin/uux-Befehl
  Beschreibung, 582
  uucico-Ausführung durch, 580
/usr/bin/vacation-Befehl, 368, 378
/usr/bin-Verzeichnis, Inhalt des, 367
/usr/dt/bin/dtmail-Mail-Benutzeragent, 373
/usr/kvm-Verzeichnis, durch Clients ohne lokalen Massenspeicher einhängen, 77
/usr/lib/inet/xntpd-Dämon, Beschreibung, 70
/usr/lib/nca_addr.so-Bibliothek, 64
/usr/lib/net/ncaconfd-Befehl, 64
/usr/lib/uucp/uucheck Befehl, 595
/usr/lib/uucp/uucheck-Befehl, 582
/usr/lib/uucp/uucleanup-Befehl, 581
/usr/lib/uucp/Uutry Befehl, 593, 594
/usr/lib/uucp/Uutry-Befehl, 582
/usr/lib-Verzeichnis, Inhalt, 372
/usr/ntp/ntpstats-Verzeichnis, 70
/usr/sbin/editmap-Befehl, 373
/usr/sbin/etrn-Skript, 373
/usr/sbin/in.comsat-Dämon, 373
/usr/sbin/inetd-Dämon, in.uucpd aufgerufen durch, 581
/usr/sbin/makemap-Befehl, 373
/usr/sbin/mount-Befehl, *Siehe* mount Befehl
/usr/sbin/newaliases-Verknüpfung, 373
/usr/sbin/ntpdate-Befehl, 70
/usr/sbin/ntpq-Befehl, 70
/usr/sbin/ntptrace-Befehl, 70

/usr/sbin/shareall-Befehl
Siehe auch shareall-Befehl
automatische gemeinsame Nutzung von Dateisystemen, 87
WebNFS-Service aktivieren, 88
/usr/sbin/showmount-Befehl, 178
/usr/sbin/sppptun-Befehl, Definition, 560
/usr/sbin/syslogd-Befehl, 373
/usr/sbin/unshareall-Befehl, 178
/usr/sbin/xntpdc-Befehl, 70
/usr-Verzeichnis, durch Clients ohne lokalen Massenspeicher einhängen, 77
uucheck Befehl, 595
uucheck-Befehl, 582
uucico-Dämon
Beschreibung, 580
Dialcodes-Datei und, 617
maximale Anzahl von gleichzeitigen Ausführungen, 583
mehrere oder verschiedene Konfigurationsdateien, 583, 597, 617
Systems-Datei und, 597
Systems-Listen ausgeben, 618
uusched-Dämon und, 581
Uutry-Befehl und, 582
uucico Dämon
Hinzufügen von UUCP-Anmeldungen, 586, 587
maximale gleichzeitige Ausführungen, 632
uucleanup-Befehl, 581
UUCP
Anmelde-Shell, 580
Anmeldungen
Hinzufügen, 586, 587
Privilegien, 625, 626
Aufrufen von Remote-Rechnern, 628
Benutzerbefehle, 582
Beschreibung, 579, 597
Callback-Option, 623
Dämonen
Übersicht, 580, 581
Dateiübertragungen
Arbeitsdateien (C.), 633, 634
Berechtigungen, 620, 623
Dämon, 580
UUCP, Dateiübertragungen *(Fortsetzung)*
Fehlerbehebung, 594
Fehlersuche, 592
Datenbankdateien, 583, 632
asppp-Konfiguration, 584
Beschreibung, 583, 584
grundlegende Konfigurationsdateien, 584
mehrere oder verschiedene Dateien, 583, 597, 617
Fehlerbehebung, 592, 638
ASSERT-Fehlermeldungen, 594, 635, 636
Befehle für die Fehlerbehebung, 595
fehlerhafte ACU, 592
fehlerhaftes Modem, 592
Prüfen der Systems-Datei, 594
Prüfen von Fehlermeldungen, 594
Prüfen von grundlegenden Informationen, 595
STATUS-Fehlermeldungen, 594, 636, 638
Suche nach Übertragungsfehlern, 594
Überprüfen von Fehlermeldungen, 638
Fehlersuche
Suche nach Übertragungsfehlern, 592
Hardwarekonfigurationen, 579
Knotenname
Alias, 583, 621
Remote-Computer, 598, 618
Konfigurieren
Ausführen von UUCP über TCP/IP, 589
Hinzufügen UUCP-Anmeldungen, 587
Hinzufügen von UUCP-Anmeldungen, 586
konfigurieren
UUCP über TCP/IP ausführen, 590
Mailansammlung, 591
manuelles Außerkraftsetzen von Parametern, 628
passiver Modusmode, 621
privilegierte Anmeldungen und Passwörter, 625, 626
Protokolldateien
anzeigen, 581
Entfernen, 589
Protokolldateien anzeigen, 581
Remote-Ausführung
Arbeitsdateien (C.), 633, 634
Befehle, 620, 623, 626

UUCP, Remote-Ausführung *(Fortsetzung)*
Dämon, 581
Remote-Computer aufrufen, 583
Shell-Skripten, 587, 589
Sicherheit
COMMANDS-Option der `Permissions`-Datei, 623, 625
Einrichten, 590
Sticky-Bit Dateien in öffentlichen Verzeichnissen, 591
VALIDATE-Option der `Permissions`-Datei, 625, 626
Solaris-Version, 579, 597
spool
cleanup-Befehl, 581
Definitionen für Jobklassen, 628, 631
Planungsdämon, 581
STREAMS-Konfiguration, 631
Übertragungsgeschwindigkeit, 600, 608
Verwalten von öffentlichen Verzeichnissen, 591
Verwaltung, 591, 592
Verwaltungsbefehle, 581, 582
Verwaltungsdateien, 633, 634
Verzeichnisse
Fehlermeldungen, 594
Verwalten von öffentlichen Verzeichnissen, 591
Verwaltung, 581
Weiterleitung, 627
UUCP (Befehl zum Kopieren von UNIX zu UNIX), Verbindung prüfen, 344
UUCP (UNIX-to-UNIX Copy Command), Mailer, 357
UUCP-Arbeitsdateien (C.)
Beschreibung, 633, 634
Entfernen, 589
UUCP-Arbeitsdateien (X.), Entfernen, 589
UUCP-Ausführungsdateien (.X), Entfernen, 589
UUCP-Ausführungsdateien (X.)
Beschreibung, 634
Entfernen, 589
`uucp` Befehl
Berechtigungen für die Weiterleitung, 627
`uucp`-Befehl
Beschreibung, 582
`uucp`-Befehl *(Fortsetzung)*
Home-Verzeichnis der Anmelde-ID, 581
`uucp` Befehl
Suche nach Übertragungsfehlern, 593
`uucp`-Befehl
`uucico`-Ausführung durch, 580
UUCP-Datendateien (D.), Entfernen, 589
UUCP-Sperrdateien (LCK), 633
`uucppublic` Verzeichnisverwaltung, 591
`uudemon.admin`-Shell-Skript, 589
`uudemon.cleanup`-Shell-Skript, 589
`uudemon.crontab`-Datei, 587
`uudemon.hour`-Shell-Skript
Beschreibung, 588
`uusched`-Dämonausführung durch, 581
`uuxqt`-Dämonausführung durch, 581
`uudemon.poll`-Shell-Skript, 588, 628
`uudirect`-Schlüsselwort des Felds "DTP", 608
`uulog` Befehl, 595
`uulog`-Befehl, 581
`uuname` Befehl, 595
`uupick`-Befehl, Beschreibung, 582
`uupick` Befehl, Entfernen von Dateien aus dem öffentlichen Verzeichnis, 592
`uusched`-Dämon
Beschreibung, 581
maximale Anzahl von gleichzeitigen Ausführungen, 583
`uudemon.hour`-Shell-Skriptaufruf, 588
`uusched` Dämon
maximale gleichzeitige Ausführungen, 632
`uustat`-Befehl, Beschreibung, 582
`uustat` Befehl
Überprüfen von Modems oder ACUs, 592
`uudemon.admin`-Shell-Skript für, 589
`uuto`-Befehl
Beschreibung, 582
`uuto` Befehl, Entfernen von Dateien aus dem öffentlichen Verzeichnis, 592
`uuto`-Befehl
`uucico`-Ausführung durch, 580
`Uutry` Befehl, 593, 594
`Uutry`-Befehl, 582

uux-Befehl
  Beschreibung, 582
  uucico-Ausführung durch, 580
uuxqt-Dämon
  Beschreibung, 581
  maximale Anzahl von gleichzeitigen Ausführungen, 583
  uudemon.hour-Shell-Skriptaufruf, 588
uuxqt Dämon
  maximale gleichzeitige Ausführungen, 632

V

-V-Option, umount-Befehl, 169
-v-Option, automount-Befehl, 131
-v Option, uucheck Befehl, 595
vacation-Befehl, 367, 368, 378
VALIDATE-Option der Permissions-Datei, 625, 626
  COMMANDS-Option, 623, 625
/var/mail-Datei, 360
/var/mail-Verzeichnis, 301, 303
  automatisches Einhängen des, 307
  Mailclientkonfiguration und, 307
/var/nca/log-Datei, 64
/var/ntp/ntp.drift-Datei, 70
/var/run/nca_httpd_1.door-Datei, 64
/var/run/sendmail.pid-Datei, 374
/var/spool/clientmqueue-Verzeichnis, 373
/var/spool/mqueue-Verzeichnis, 373
/var/spool/uucppublic Verzeichnisverwaltung, 591
/var/uucp/.Admin/errors Verzeichnis, 594
/var/uucp/.Status-Verzeichnis, 594
Variablen in Map-Einträgen, 227
Veraltete Services (SLP)
  Advertisement, 281, 286
  Definition, 281
Verbindungsarten im PPP
  physische Verbindungsmedien, 425
  Standleitung, 429
  Teile einer Verbindung, 425
  Vergleich von Wählverbindungen und Standleitungsverbindungen, 429
  wählen, 425
Verifizieren, Remote-Systembetrieb, 686
Vermeiden von Problemen mit Zugriffssteuerungslisten in NFS, 199
Verschlüsselte Zuordnungsdatei, erstellen, 333
Verschlüsselung mit öffentlichen Schlüsseln
  allgemeiner Schlüssel, 211
  Datenbank mit öffentlichen Schlüsseln, 210
  DH-Authentifizierung, 210, 211
  Dialogschlüssel, 211
  geheimer Schlüssel
    Datenbank, 210
    vom Remote-Server löschen, 211
  zu Zeitsynchronisierung, 211
Verschlüsselung mit öffentlichen Schlüssseln, Datenbank mit öffentlichen Schlüsseln, 209
Versionsaushandlung, NFS, 187–188
Versionsstand, Angeben in sendmail.cf-Datei, 354
Vertrauenswürdige Anrufer, für CHAP-Authentifizierung konfigurieren, 491
Vertrauenswürdige Netzwerkumgebung
  Remote-Anmeldung
    Authentifizierungsprozess, 681
    Vorgang nach dem Anmelden, 684
vertrauenswürdige Netzwerkumgebung
  Remote-Anmeldung
    Vorgang nach dem Anmelden, 684
vertrauenswürdiges aufrufendes Programm, 432
Verwalten von öffentlichen Verzeichnissen (UUCP), 591
Verwalten von UUCP
  Hinzufügen von Anmeldungen, 586, 587
  Mail, 591
  öffentliches Verzeichnis, 591
  reguläre Verwaltung, 591, 592
  Shell-Skripten, 587, 589
Verwaltungsbefehle (UUCP), 581, 582
Verwaltungsdateien (UUCP)
  Arbeitsdateien (C.), 633, 634
  Ausführungsdateien (X.), 581, 634
  Entfernen, 589
  Sperrdateien (LCK), 633
  temporäre Datendateien (TM), 633
Verzeichnisagent (SLP)
  DA-Adressen, 253
  Lastausgleich, 273–274

Verzeichnisagent (SLP) *(Fortsetzung)*
Netzwerküberlastung und, 257
SLP-Architektur und, 238
wann eine Bereitstellung erforderlich ist, 272
wo eine Bereitstellung erforderlich ist, 273–274
Verzeichnisse (UUCP)
Fehlermeldungen, 594
Verwalten von öffentlichen Verzeichnissen, 591
Verwaltung, 581
Verzögerungs-Escape-Zeichen, 614
`vfstab`-Datei
`automount`-Befehl und, 219
clientseitigen Failover aktivieren, 94
Dateisysteme während des Boot-Vorgangs einhängen, 91
durch Clients ohne lokalen Massenspeicher einhängen, 77
NFS-Server und, 91
`nolargefiles`-Option, 93
Virtuelle Hosts, Einrichten, 315
`VIRTUSER_DOMAIN_FILE()`
`m4`-Konfigurationsmakro, 408
`VIRTUSER_DOMAIN()` `m4`-Konfigurationsmakro, 408
`virtuser_entire_domain`
`FEATURE()`-Deklaration, 411
Vorlagendateien (PPP)
`/etc/ppp/myisp-chat.tmpl`, 541–542
`/etc/ppp/options.tmpl`, 530
`/etc/ppp/peers/myisp.tmpl`, 536
`options.ttya.tmpl`, 533
Vorlagendateien, 457

W

Wagenrücklauf-Escape-Zeichen, 614
Wählcodekürzel, 583, 601
Wählverbindung
allgemeine Probleme diagnostizieren
Netzwerk, 510
serielle Verbindungen, 519
Authentifizierung für die Verbindung, 432
Chat-Skripten
Beispiel, 539–541, 542–543, 546
für einen ISDN TA, 545–546
Wählverbindung *(Fortsetzung)*
Chat-Skripten erstellen, 538
Definition, 425
Diagnostizierung allgemeiner Probleme mit `pppd`, 507
Planung, 438
Teile der Verbindung, 426–428
Wählvorgang, 428
WAN (Wide Area Network)
Usenet, 579, 597
WARNING: mountpoint already mounted on (Meldung), 132
Warteschlange (UUCP)
cleanup-Befehl, 581
Definitionen für Jobklassen, 628, 631
Planungsdämon, 581
Spool-Verzeichnis, 633
`uusched`-Dämon
Beschreibung, 581
maximale Anzahl von gleichzeitigen Ausführungen, 583
`uusched` Dämon
maximale gleichzeitige Ausführungen, 632
Verwaltungsdateien, 633, 634
Warteschlangenfunktionen ab Version 8.12, `-sendmail` Befehl, 414
WebNFS-Service
aktivieren, 88
Beschreibung, 206–207
Firewalls und, 107
planen für, 105–106
Sicherheitsaushandlungen und, 83
suchen, 106–107
Übersicht, 82
Übersicht der Schritte, 104
URL-Servicetypen und, 106
Weiterleitung (UUCP), 627
WRITE-Option der `Permissions`-Datei, 622

X

X. UUCP-Ausführungsdateien, `uuxqt`-Ausführung, 581
`xntpd`-Dämon, 68, 70

`xntpdc`-Befehl, 70
`xonxoff`-Option (PPP), 468

Z

Zeilenvorschub-Escape-Zeichen, 614
Zeit
  mit einem anderen System synchronisieren, 69
Zeitsynchronisierung, 211
Zeitüberschreitungen (SLP), 262, 263, 271
Zugangsserver (PPP)
  Befehle und Dateien zum Konfigurieren, 561, 562–564
  Definition, 434
  eine Schnittstelle auf PPPoE-Clients beschränken, 502
  `/etc/ppp/chap-secrets`-Datei, 566
  `/etc/ppp/options`-Datei, 566
  `/etc/ppp/pap-secrets`-Datei, 566
  konfigurieren, für PPPoE, 500, 501, 564–566
  Übersicht der Schritte für die Planung, 451
  Übersicht der Schritte zum Konfigurieren, 495–496
Zugriffskontrollliste (ACL) und NFS
  Beschreibung, 80, 197–199
  Fehlermeldung, `Permission denied`, 139